CA Infrastructure Management Data Aggregator

Manuel de l'administrateur

Version 2.3.4

La présente documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA.

La présente Documentation ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA. La présente Documentation est confidentielle et demeure la propriété exclusive de CA. Elle ne peut pas être utilisée ou divulguée, sauf si (i) un autre accord régissant l'utilisation du logiciel CA mentionné dans la Documentation passé entre vous et CA stipule le contraire ; ou (ii) si un autre accord de confidentialité entre vous et CA stipule le contraire.

Nonobstant ce qui précède, si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2014 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Produits CA Technologies référencés

Ce document fait référence aux produits CA Technologies suivants :

- CA Infrastructure Management Data Aggregator (Data Aggregator)
- CA Infrastructure Management Data Collector (Data Collector)
- CA Performance Center

Support technique

Pour une assistance technique en ligne et une liste complète des sites, horaires d'ouverture et numéros de téléphone, contactez le support technique à l'adresse http://www.ca.com/worldwide.

Table des matières

Chapitre 1: Administration de produit 9

Procédure de configuration des sauvegardes automatiques de Data Repository (installations à noeud unique et en cluster) 10
Remarques concernant la sauvegarde de Data Repository 10
Configuration d'une sauvegarde de Data Repository vers un hôte distant (installations à noeud unique et en cluster) 11
Configuration d'une sauvegarde de Data Repository vers le même hôte (installations à noeud unique et en cluster) 14
Configuration de Data Repository 15
Restauration du Data Repository 19
Sauvegarde de Data Aggregator 22
Restauration de Data Aggregator 24
Affichage des détails de Data Aggregator 25
Affichage de la liste des installations de Data Collector 25
Gestion des installations de Data Collector 26
Rééquilibrage de la charge sur Data Collector 28
Equilibrage de la charge pour des Data Collector qui extraient des données non-SNMP (CAMM) 29
Procédure de déplacement de Data Collector vers un autre hôte 30
Déterminez l'identificateur unique pour Data Collector. 33
Arrêtez Data Collector. 33
Installation de Data Collector sur un autre hôte 35
Changements de configuration de Data Aggregator en cas de déconnection réseau d'un hôte Data Collector 37
Mise en cache Data Collector des données interrogées lorsque l'hôte Data Aggregator est indisponible 37
Calcul de la mémoire requise pour la mise en cache des données d'interrogation 38
Modification de la limite de mémoire du cache de données 39
Processus d'audit du Data Repository 40
Processus de surveillance du signal d'activité de Data Repository 41
Choix d'autre hôte dans un cluster en cas de panne de l'hôte sélectionné 42
Modification l'utilisation maximum de la mémoire pour les composants Data Aggregator et Data Collector après l'installation (facultatif) 44
Modification de la limite de mémoire externe d'ActiveMQ après l'installation (facultatif) 46
Gestion de la conservation de données 48

Chapitre 2: Redémarrage des services de composants 51

Arrêt et redémarrage du Data Aggregator 51
Arrêt et redémarrage de Data Collector 53

Arrêt et redémarrage du Data Repository 54
Arrêt et redémarrage de l'intermédiaire ActiveMQ 56

Chapitre 3: Détection de votre réseau 59

Détection d'unités 59
Flux de travaux de détection 60
Profils SNMP 62
Détection et interrogation 63
Détection et interrogation dans des environnements VMware 66
Profils de détection 66
Affichage d'une liste de profils de détection 68
Création de profils de détection 68
Modification des profils de détection 73
Suppression des profils de détection 76
Exécution de détections à la demande 76
Détections de planification 78
Affichage des résultats de la détection 79
Détection à partir d'autres sources de données 81
Modifications du type d'unité 82
Nouvelle détection 84

Chapitre 4: Gestion de l'infrastructure 85

Personnalisation du flux de travaux de gestion des unités et des composants 85
Profils de surveillance 88
Associations de profils de surveillance prédéfinis 89
Affichage des profils de surveillance 90
Assignation ou suppression des profils de surveillance des collections d'unités 92
Collections d'unités prédéfinies 93
Collection d'unités All Devices (Toutes les unités) 95
Collection d'unités All Routers (Tous les routeurs) 95
Collection d'unités All Servers (Tous les serveurs) 95
Collection d'unités All Switches (Tous les commutateurs) 96
Collection d'unités All Manageable Devices (Toutes les unités gérables) 96
Collection d'unités All ESX Hosts (Tous les hôtes ESX) 97
Collection d'unités All Virtual Machines (Toutes les machines virtuelles) 97
Collection d'unités All VMware vCenters (Tous les serveurs VMware vCenters) 97
Collections d'unités personnalisées 98
Affichage des unités surveillées 99
Suppression d'unités 102
Modification de l'adresse IP principale d'une unité surveillée 103
Suppression des composants retirés 103

Suppressions de domaine IP 106
Suppressions de client hébergé 107
Désactivation des clients hébergés 107
Activation des clients hébergés 109
Reconfiguration des unités 110
Gestion de la détection des modifications 110
Mise à jour automatique de la reconfiguration des unités 113
Mise à jour manuelle de la reconfiguration des unités 114

Chapitre 5: Gestion des interfaces 117

Interrogation des interfaces critiques plus rapide que celles des interfaces non critiques 117
Affichage des profils de surveillance 119
Copie d'un profil de surveillance prédéfini 120
Définition d'un filtre d'interface 122
Remarques concernant les filtres d'interface et les profils de surveillance multiples 123
Affectation d'un profil de surveillance à une collection d'unités 125
Affichage des unités surveillées pour vérifier les résultats 126
Méthode de définition et d'activation d'un filtre d'interface 129
Suppression d'un filtre d'interface 131
Convention d'attribution de nom de composants d'interface 132
Calcul de l'utilisation de l'interface 132
Remplacement des valeurs de vitesse en entrée et de vitesse en sortie au niveau des interfaces 132

Chapitre 6: Génération d'événements 135

Instructions concernant les performances des événements 135
Méthode de surveillance du traitement des événements 136
Méthode de correction en cas de dépassement du seuil 137
Evénements de gestion des performances 138
Références moyennes 138
Procédure de surveillance des performances d'unité à l'aide d'événements 139
Surveillance des mesures à l'aide de règles d'événement 141
Création d'une collection d'unités personnalisée 142
Ajout de règles à une collection d'unités personnalisée 143
Création d'un profil de surveillance et ajout de règles d'événement 144
Affectation d'un profil de surveillance à une collection d'unités personnalisée 148
Affichage des événements 149
Procédure de configuration des notifications à partir du gestionnaire d'événements 150
Types d'événements 153

Chapitre 7: Reporting 155

Utilisation des filtres 155
Références moyennes 156
95e centile 157
Ecart type 157
Valeurs minimum et maximum 158

Annexe A: Calculs 159

Calculs de moyenne de référence 159
Calculs du 95e centile 164
Calculs d'écart standard 166

Annexe B: Dépannage 169

Dépannage : la détection ne démarre pas 169
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée 170
Dépannage : message d'événement d'arrêt de l'interrogation 171
Dépannage : l'interrogation ne termine pas pour une unité primordiale 171
Dépannage : modification de l'adresse IP de Data Aggregator requise pour la modification de mon environnement 172
Dépannage : arrêt inattendu de Data Aggregator 172
Dépannage : je ne parviens pas à sauvegarder le Data Repository. 174
Dépannage : Déclenchement d'alarmes d'intrusion en cas de présence de plusieurs unités SNMP 175

Glossaire 177

Chapitre 1: Administration de produit

Ce chapitre traite des sujets suivants :

Procédure de configuration des sauvegardes automatiques de Data Repository (installations à noeud unique et en cluster) (page 10)
Restauration du Data Repository (page 19)
Sauvegarde de Data Aggregator (page 22)
Restauration de Data Aggregator (page 24)
Affichage des détails de Data Aggregator (page 25)
Affichage de la liste des installations de Data Collector (page 25)
Gestion des installations de Data Collector (page 26)
Rééquilibrage de la charge sur Data Collector (page 28)
Equilibrage de la charge pour des Data Collector qui extraient des données non-SNMP (CAMM) (page 29)
Procédure de déplacement de Data Collector vers un autre hôte (page 30)
Changements de configuration de Data Aggregator en cas de déconnection réseau d'un hôte Data Collector (page 37)
Mise en cache Data Collector des données interrogées lorsque l'hôte Data Aggregator est indisponible (page 37)
Processus d'audit du Data Repository (page 40)
Processus de surveillance du signal d'activité de Data Repository (page 41)
Choix d'autre hôte dans un cluster en cas de panne de l'hôte sélectionné (page 42)
Modification l'utilisation maximum de la mémoire pour les composants Data Aggregator et Data Collector après l'installation (facultatif) (page 44)
Modification de la limite de mémoire externe d'ActiveMQ après l'installation (facultatif) (page 46)
Gestion de la conservation de données (page 48)

Procédure de configuration des sauvegardes automatiques de Data Repository (installations à noeud unique et en cluster)

Dans certains cas, vous devrez sauvegarder le Data Repository. Par exemple, vous pouvez sauvegarder le Data Repository avant de mettre à niveau le Data Aggregator ou avant de configurer des sauvegardes automatiques par l'intermédiaire d'un job cron. La sauvegarde du Data Repository vous fournit une copie du Data Repository que vous pouvez utiliser en cas d'erreur imprévue.

Important : La première sauvegarde du Data Repository est de type complète. Elle peut prendre beaucoup de temps si la quantité de données historiques présentes est volumineuse. Une fois la sauvegarde initiale effectuée, les sauvegardes planifiées ultérieures sont de type incrémentielles. En cas de sauvegarde quotidienne, une sauvegarde incrémentielle doit signaler l'activité ayant eu lieu au niveau de la base de données uniquement pour les dernières 24 heures (par exemple, la durée qui s'est écoulée depuis la dernière sauvegarde).

Pour effectuer une sauvegarde incrémentielle après une sauvegarde complète, spécifiez le script de sauvegarde Vertica avec le même paramètre snapshotName et le même répertoire de sauvegarde indiqués lors de la sauvegarde complète. Si vous modifiez ces noms, une sauvegarde complète sera effectuée.

Vertica (la base de données) crée les fichiers de données dans lesquels les données seront stockées. Ces fichiers ne sont jamais modifiés après avoir été créés ; des nouveaux sont créés et les anciens sont supprimés. Cette approche permet de profiter de l'utilitaire de resynchronisation standard pour la réplication rapide des fichiers vers un autre ordinateur dans le cadre de la sauvegarde du Data Repository. Pour plus d'informations sur l'utilitaire rsync, consultez le site http://everythinglinux.org/rsync/.

Pour configurer les sauvegardes automatiques de Data Repository, procédez comme suit :

1. Consultez les remarques concernant la sauvegarde (page 10).
2. Effectuez l'une des opérations suivantes :
   - Configurez une sauvegarde de Data Repository vers un hôte distant (page 11).
   - Configurez une sauvegarde de Data Repository sur le même hôte (page 14).
3. Configurez Data Repository (page 15).

Remarques concernant la sauvegarde de Data Repository

Tenez compte des informations suivantes avant de sauvegarder Data Repository :

- Vous n'êtes pas obligé d'arrêter Data Repository ou Data Aggregator lorsque vous sauvegardez Data Repository.

- Les sauvegardes sont stockées à l'emplacement spécifié dans le fichier de configuration que vous utilisez pour sauvegarder la base de données. Le répertoire contenant le fichier de sauvegarde contient un sous-répertoire pour chaque noeud qui est sauvegardé à cet emplacement. Le sous-répertoire contient un répertoire avec le nom du cliché de sauvegarde. Le nom de cliché est défini à l'aide de l'option snapshotName dans le fichier de configuration.
- Effectuez des sauvegardes incrémentielles de façon quotidienne. Nous vous recommandons d'effectuer des sauvegardes pendant les heures non ouvrées, car le traitement de sauvegarde requiert une grande quantité de ressources.
- Vous pouvez sauvegarder Data Repository sur un hôte distant ou sur le même hôte.

  Remarque : Si vous effectuez une sauvegarde sur le même hôte, enregistrez-la dans une partition différente de celle utilisée par les répertoires de catalogues et de données.
- Effectuez des sauvegardes complètes chaque semaine. Les clichés quotidiens dépendent de la sauvegarde complète. Effectuer une restauration vers un cliché dépend de l'intégrité de la sauvegarde complète. Tenez compte des informations suivantes concernant les sauvegardes complètes :
  - Créez un fichier .ini pour chaque sauvegarde complète hebdomadaire. Le fichier .ini est requis pour effectuer une restauration vers un cliché particulier. Lorsqu'un nom unique est donné au fichier INI et que ce fichier est exécuté pour la première fois, une sauvegarde complète est effectuée. Par conséquent, il est important de considérer l'espace disque disponible. Si peu d'espace disque est disponible, il est recommandé de conserver uniquement une ou deux semaines de données, en plus de la semaine actuelle. Cette solution requiert une opération de maintenance supplémentaire pour supprimer la semaine de sauvegardes la plus ancienne, chaque fois qu'une nouvelle semaine commence.
  - Effectuez une sauvegarde complète à l'aide de la commande /opt/vertica/bin/vbr.py -setupconfig pour générer un nouveau fichier INI ou au moyen d'une copie de la version actuelle de ce fichier. Copiez le fichier INI existant dans un nouveau fichier INI, puis modifiez la valeur de snapshotName dans ce nouveau fichier.

Informations complémentaires :

Procédure de configuration des sauvegardes automatiques de Data Repository (installations à noeud unique et en cluster) (page 10)

Configuration d'une sauvegarde de Data Repository vers un hôte distant (installations à noeud unique et en cluster)

Vous pouvez sauvegarder Data Repository sur un hôte distant.

Nous vous recommandons d'associer à chaque noeud Data Repository un hôte distant unique de stockage des sauvegardes. Par exemple, pour un environnement de cluster incluant trois noeuds Data Repository, chaque hôte Data Repository doit posséder un hôte de sauvegarde dédié.

Important : Pour les environnements de cluster, effectuez les opérations suivantes sur chaque hôte distant que vous envisagez d'utiliser pour la sauvegarde de *chaque* noeud de cluster. Vous devez sauvegarder tous les noeuds inclus dans le cluster.

Procédez comme suit :

1. Ouvrez une console et connectez-vous en tant qu'utilisateur root à l'ordinateur que vous souhaitez utiliser comme hôte de sauvegarde distant :
2. Pour créer l'administrateur de base de données Vertica Linux sur l'hôte de sauvegarde distant, saisissez la commande suivante :

   ```
   useradd administrateur_BdD -s /bin/bash
   ```

   Par exemple :

   ```
   useradd dradmin -s /bash/bin
   ```

   Remarque : Créez le même administrateur de base de données Vertica Linux sur l'hôte de sauvegarde distant que celui qui existe sur l'hôte de Data Repository. Vérifiez que l'hôte de Data Repository et l'hôte de sauvegarde distant ne sont pas connectés à une connexion LDAP ou NIS (Network Information Service) et qu'ils partagent le même administrateur de base de données Vertica Linux.
3. Pour définir le mot de passe d'administrateur de base de données Vertica Linux, saisissez la commande suivante :

   ```
   passwd administrateur_BdD
   ```

   Par exemple :

   ```
   passwd dradmin
   ```
4. Pour créer des répertoires Vertica sur l'hôte de sauvegarde distant, saisissez les commandes suivantes :

   ```
   mkdir /opt/vertica/bin
   ```

   ```
   mkdir /opt/vertica/oss
   ```
5. Pour remplacer le propriétaire des répertoires Vertica, saisissez la commande suivante :

   ```
   chown -R dradmin /opt/vertica
   ```
6. Déconnectez-vous de l'hôte de sauvegarde distant.
7. Pour configurer une connexion ssh sans mot de passe sur l'hôte Data Repository pour l'hôte de sauvegarde distant, procédez comme suit :
   a. Ouvrez une console et connectez-vous à l'hôte de Data Repository en tant qu'administrateur de base de données Vertica Linux.

b. Saisissez les commandes suivantes :

```
ssh-keygen -N " -t rsa -f ~/.ssh/id_rsa
cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys2
chmod 644 ~/.ssh/authorized_keys2
```

c. Pour copier la clé publique de l'administrateur de la base de données dans la liste des clés autorisées de l'hôte de sauvegarde distant, saisissez la commande suivante :

```
ssh-copy-id -i dradmin@backuphost
```

d. Ouvrez une console et connectez-vous à l'hôte de sauvegarde distant en tant qu'administrateur de la base de données Vertica Linux.

e. Pour copier les outils rsync et python de Vertica à partir de l'hôte de Data Repository sur l'hôte de sauvegarde distant, saisissez les commandes suivantes :

```
scp dradmin@<drhost>:/opt/vertica/bin/rsync /opt/vertica/bin
scp -r dradmin@<drhost>:/opt/vertica/oss/python /opt/vertica/oss
```

8. Vérifiez que l'hôte de sauvegarde distant comprend les nouveaux répertoires de fichiers /opt/vertica/bin/rsync et /opt/vertica/oss/python.

9. Pour créer le répertoire de sauvegarde sur l'hôte de sauvegarde distant, saisissez la commande suivante :

```
mkdir répertoire_sauvegarde
```

répertoire_sauvegarde

Indique le répertoire dans lequel vous souhaitez sauvegarder le Data Repository. Sélectionnez un répertoire de sauvegarde qui est sur une partition de disque avec une grande quantité d'espace disponible. Si ces répertoires ne sont pas accessibles en écriture par l'administrateur de base de données, octroyez cet accès utilisateur à ces répertoires via les commandes chown et chmod.

Remarque : Dans une installation de cluster, créez les répertoires de sauvegarde avant de sauvegarder la base de données. Vous pouvez choisir un répertoire de sauvegarde différent pour chaque hôte.

Par exemple :

```
mkdir ~dradmin/backups
```

Informations complémentaires :

Procédure de configuration des sauvegardes automatiques de Data Repository (installations à noeud unique et en cluster) (page 10)

Configuration d'une sauvegarde de Data Repository vers le même hôte (installations à noeud unique et en cluster)

Vous pouvez sauvegarder Data Repository sur le même hôte. Dans un environnement de cluster, vous devez sauvegarder chaque noeud inclus dans le cluster. Vous pouvez choisir un répertoire de sauvegarde différent pour chaque hôte.

Procédez comme suit :

1. Connectez-vous au Data Repository avec le compte d'utilisateur Linux de l'administrateur de base de données.

   Remarque : Dans une installation en cluster, vous pouvez vous connecter au Data Repository à partir d'un des trois hôtes membres du cluster.

2. Assurez-vous que le compte d'utilisateur Linux de l'administrateur de base de données est configuré avec une clé SSH sans mot de passe.

   Remarque : Dans une installation de cluster, assurez que les clés SSH sans mot de passe sont configurées pour *chaque* hôte qui participe au cluster.

   Procédez comme suit :

   a. Pour vérifier si une clé SSH sans mot de passe est déjà définie, tapez la commande suivante :

      ```
      ssh nom_hôte ls
      ```

      hostname

      Indique le nom de l'hôte sur lequel Data Repository est installé.

      Si la clé SSH sans mot de passe est configurée, vous *n'êtes pas invité* à saisir de mot de passe. Vous n'avez pas d'autre opération à effectuer.

   b. Si vous *êtes invité* à saisir un mot de passe, ignorez l'invite et appuyez sur Ctrl+C. Pour configurer le compte d'utilisateur Linux de l'administrateur de base de données avec une clé SSH sans mot de passe, tapez la commande :

      ```
      ssh-keygen -N " -t rsa -f ~/.ssh/id_rsa
      cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys2
      chmod 644 ~/.ssh/authorized_keys2
      ```

      Pour confirmer qu'*aucune* invite de mot de passe n'est requise pour un mot de passe, saisissez de nouveau la commande suivante :

      ```
      ssh nom_hôte ls
      ```

      hostname

      Indique le nom de l'hôte sur lequel Data Repository est installé.

   Important : Si vous ne configurez aucune clé SSH sans mot de passe, vous ne pouvez pas sauvegarder le Data Repository. Configurez une clé SSH sans mot de passe même si vous enregistrez la sauvegarde sur le même ordinateur.

3. Pour créer le répertoire de sauvegarde, saisissez la commande suivante :

   ```
   mkdir répertoire_sauvegarde
   ```

   répertoire_sauvegarde

   Indique le répertoire dans lequel vous souhaitez sauvegarder le Data Repository. Sélectionnez un répertoire de sauvegarde qui est sur une partition de disque avec une grande quantité d'espace disponible. Si ces répertoires ne sont pas accessibles en écriture par l'administrateur de base de données, octroyez cet accès utilisateur à ces répertoires via les commandes chown et chmod.

   Remarque : Dans une installation de cluster, créez les répertoires de sauvegarde avant de sauvegarder la base de données. Vous pouvez choisir un répertoire de sauvegarde différent pour chaque hôte.

   Par exemple :

   ```
   mkdir ~dradmin/backups
   ```

Informations complémentaires :

Procédure de configuration des sauvegardes automatiques de Data Repository (installations à noeud unique et en cluster) (page 10)

Configuration de Data Repository

Configurez Data Repository pour permettre les sauvegardes automatisées.

Procédez comme suit :

1. Connectez-vous au Data Repository avec le compte d'utilisateur Linux de l'administrateur de base de données.

   Remarque : Dans une installation en cluster, vous pouvez vous connecter au Data Repository à partir d'un des trois hôtes membres du cluster. Toutefois, nous vous recommandons de vous connecter à l'hôte Data Repository qui va initialiser les sauvegardes.

2. Pour créer un script de configuration réutilisable pour la sauvegarde et la restauration du Data Repository, saisissez la commande suivante comme compte d'utilisateur Linux pour l'administrateur de la base de données :

   ```
   /opt/vertica/bin/vbr.py --setupconfig
   ```

   Remarque : Nous vous recommandons de lancer cette commande dans le répertoire cible du fichier de configuration. Le compte d'utilisateur Linux correspondant à l'administrateur de base de données doit posséder des droits d'accès en écriture sur ce répertoire.

Vous êtes invité à fournir des réponses à diverses questions et à des instructions. Voici une liste de questions et d'instructions et une description des réponses typiques :

- Nom de l'instantané : *nom du cliché de sauvegarde*
- Sauvegardes de configurations Vertica ? [y/n]: y
- Nombre de points de restauration (1) : 7

  Remarque : La définition du nombre de points de restauration sur sept permet de restaurer la dernière sauvegarde de Data Repository ou l'une des sept sauvegardes incrémentielles précédentes de Data Repository. Si le point de restauration est défini sur un, vous pouvez restaurer uniquement la dernière sauvegarde de Data Repository ou la sauvegarde incrémentielle précédente de Data Repository. La sauvegarde la plus ancienne est supprimée lorsque la limite du nombre de points de restauration est atteinte. Si vous souhaitez conserver plusieurs points de restauration, augmentez le nombre de points de restauration ou modifiez le nom du cliché dans le fichier de configuration. Toutefois, la modification du nom du cliché lance une nouvelle série de sauvegardes complètes, ce qui peut doubler la quantité d'espace disque requise pour les sauvegardes.
- Spécifiez des objets (aucune valeur par défaut) : ne spécifiez pas de valeur et appuyez sur la touche Retour pour garantir la sauvegarde de tous les objets.
- Nom d'utilisateur Vertica (dradmin) : acceptez la valeur par défaut en appuyant sur la touche Retour.
- Enregistrer le mot de passe pour éviter l'apparition de l'invite lors de l'exécution ? (n) [y/n]: y
- Mot de passe à enregistrer dans le fichier de configuration vbr (aucune valeur par défaut) : entrez le mot de passe lorsque vous y êtes invité.

  Remarque : Ce mot de passe doit correspondre au mot de passe de base de données pour le compte d'administrateur de base de données au niveau de la base de données Vertica.
- Nom d'hôte de sauvegarde (aucune valeur par défaut) : *nom de l'hôte de sauvegarde*

  Remarque : Si vous sauvegardez un cluster, une invite s'affiche vous demandant d'indiquer le nom d'hôte correspondant à chaque noeud dans le cluster. Vous devez sauvegarder chaque noeud inclus dans le cluster.
- Répertoire de sauvegarde (aucune valeur par défaut) : *chemin du répertoire de sauvegarde du Data Repository*

  Remarque : Si vous sauvegardez un cluster, vous devez indiquer un répertoire de sauvegarde pour chaque noeud dans le cluster. Vous devez sauvegarder chaque noeud inclus dans le cluster.

- Nom du fichier de configuration (cliché name.ini) : acceptez la valeur par défaut en appuyant sur la touche Retour.

  Vérifiez que vous possédez des droits d'accès en écriture sur le répertoire dans lequel vous créez le fichier INI. Si vous n'entrez pas le chemin complet du fichier INI, le fichier est enregistré dans le répertoire à partir duquel vous avez exécuté la commande /opt/vertica/bin/vbr.py --setupconfig.

  Important : Le fichier de configuration généré contient un mot de passe en texte clair.

- Modifier les paramètres avancés ? (n) [y/n]:n

  Un message s'affiche, indiquant que la configuration de vbr a été enregistrée dans un fichier de configuration nommé name.ini.

3. Sauvegardez Data Repository. Saisissez la commande suivante :

   ```
   /opt/vertica/bin/vbr.py --task backup --config-file
   nom_fichier_chemin_accès_répertoire_configuration
   ```

   nom_fichier_chemin_accès_répertoire_configuration

   Indique le nom de fichier et le chemin d'accès du répertoire du fichier de configuration que vous avez créé préalablement. Ce fichier se situe à l'emplacement où vous avez exécuté l'utilitaire de sauvegarde (/opt/vertica/bin/vbr.py).

   Par exemple :

   ```
   /opt/vertica/bin/vbr.py --task backup --config-file
   /home/vertica/vert-db-production.ini
   ```

   Remarque : Si vous êtes invité à confirmer l'authenticité de l'hôte, répondez yes.

   Remarque : Dans une installation en cluster, vous devez uniquement effectuer cette étape avec un des hôtes qui participent au cluster.

   Le Data Repository est sauvegardé.

4. (Facultatif) Si vous ne voulez pas conserver le mot de passe en texte clair du Data Repository pour les prochaines sauvegardes manuelles, suivez les étapes suivantes :

   a. Vérifiez que la ligne suivante existe dans la section [Database] :

      ```
      dbPromptForPassword = True
      ```

   b. Supprimez la ligne suivante de la section [Database] :

      ```
      dbPassword = mot_de_passe
      ```

   Remarque : Pour effectuer des sauvegardes automatisées, la ligne dbPassword doit rester dans le fichier de configuration avec le mot de passe correspondant. Définissez dbPromptForPassword sur False.

5. Pour configurer une sauvegarde quotidienne automatisée (recommandée) du Data Repository, procédez comme suit :

   a. Pour créer un script Shell d'encapsulateur, ouvrez votre éditeur de texte.

b. Le contenu du script Shell d'encapsulateur doit contenir la ligne unique suivante :

```
/opt/vertica/bin/vbr.py --task backup --config-file
nom_fichier_chemin_accès_répertoire_configuration
```

nom_fichier_chemin_accès_répertoire_configuration

Indique le nom de fichier et le chemin d'accès du répertoire du fichier de configuration que vous avez créé préalablement. Ce fichier se situe à l'emplacement où vous avez exécuté l'utilitaire de sauvegarde (/opt/vertica/bin/vbr.py).

Par exemple :

```
/opt/vertica/bin/vbr.py --task backup --config-file
/home/vertica/vert-db-production.ini
```

c. Enregistrez le contenu dans un nouveau fichier nommé backup_script.sh à l'emplacement de votre choix.

Par exemple :

```
/home/vertica/backup_script.sh
```

d. Modifiez les autorisations d'exécution du script en saisissant la commande suivante :

```
chmod 777 emplacement_backup_script.sh/backup_script.sh
```

Par exemple :

```
chmod 777 /home/vertica/backup_script.sh
```

e. Pour utiliser le compte d'utilisateur Linux pour l'administrateur de base de données, saisissez la commande suivante :

```
crontab -e
```

f. Ajoutez un job cron qui exécutera le script de sauvegarde que vous avez créé préalablement.

Remarque : Nous vous suggérons de créer un job cron pour exécuter le script tous les jours, à une heure creuse.

Par exemple :

```
00 02 * * *   /home/vertica/backup_script.sh >/tmp/backup.log  2>&1
```

Cet exemple de job cron exécutera le script de sauvegarde tous les jours à 02 h 00.

Important : La première sauvegarde du Data Repository est de type complète. Elle peut prendre beaucoup de temps si la quantité de données historiques présentes est volumineuse. Une fois la sauvegarde initiale effectuée, les sauvegardes planifiées ultérieures sont de type incrémentielles. En cas de sauvegarde quotidienne, une sauvegarde incrémentielle doit signaler l'activité ayant eu lieu au niveau de la base de données uniquement pour les dernières 24 heures (par exemple, la durée qui s'est écoulée depuis la dernière sauvegarde).

Restauration du Data Repository

Une fois le Data Repository sauvegardé, vous pouvez le restaurer. Cette procédure suppose que l'administrateur de la base de données fait partie du fichier sudoers.

Remarque : En général, vous restaurez Data Repository vers le même ordinateur qui a servi à la sauvegarde. Toutefois, vous *pouvez* restaurer Data Repository vers un ordinateur différent. L'ordinateur vers lequel vous effectuez la restauration doit être configuré de la même façon que l'ordinateur à l'origine de la sauvegarde. Dans un environnement de cluster, chaque ordinateur vers lequel vous effectuez une restauration doit être configuré de la même façon que chaque ordinateur à partir duquel vous avez sauvegardé chaque noeud de Data Repository.

Les configurations suivantes doivent être identiques :

- Adresse IP
- Nom d'hôte
- Répertoires de catalogue et de données
- Autorisations du répertoire de catalogue et de données
- Informations d'identification de l'administrateur de base de données Vertica Linux
- Informations d'identification du compte d'administrateur de la base de données
- Informations d'identification du compte d'utilisateur de la base de données

Procédez comme suit :

1. Arrêtez tous les hôtes Data Collector associés au Data Aggregator en vous connectant aux ordinateurs sur lesquels le Data Collector est installé comme utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes. Ouvrez une invite de commande et saisissez la commande suivante :

   ```
   service dcmd stop
   ```

   Les hôtes Data Collector s'arrêtent.

2. Arrêtez Data Aggregator en vous connectant à l'ordinateur sur lequel Data Aggregator est installé comme utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes. Ouvrez une invite de commande et saisissez la commande suivante :

   ```
   service dadaemon stop
   ```

   Remarque : Pour plus d'informations sur la création d'un utilisateur sudo disposant d'un accès à un ensemble limité de commandes, reportez-vous au *Manuel d'installation de Data Aggregator*.

   Le Data Aggregator s'arrête.

3. Connectez-vous au serveur de base de données que vous utilisez pour le Data Repository en tant qu'administrateur de base de données et non *pas* qu'utilisateur root :

4. Saisissez la commande suivante :

   ```
   /opt/vertica/bin/adminTools
   ```

   La boîte de dialogue Administration Tools s'affiche.

5. Sélectionnez (4) Stop Database.

6. Appuyez sur la barre d'espacement à côté du nom de la base de données, sélectionnez OK et appuyez sur Entrée.

   Vous êtes invité à entrer le mot de passe de la base de données.

7. Entrez le mot de passe de base de données et appuyez sur Entrée.

   Le Data Repository s'arrête.

   Remarque : Si Data Repository ne s'arrête pas, sélectionnez (2) Stop Vertica on Host dans (7) Advanced Tools Menu.

8. Sélectionnez Exit et appuyez sur Entrée.

9. Pour préparer la restauration de la sauvegarde du Data Repository, connectez-vous avec le compte d'utilisateur Linux de l'administrateur de base de données au serveur de base de données sur lequel se trouve le Data Repository.

   Lors de la configuration des sauvegardes automatiques de Data Repository, vous avez configuré le fichier de configuration avec un nombre de points de restauration de sept. Vous pouvez restaurer Data Repository à partir de la dernière sauvegarde ou de l'une des sept sauvegardes incrémentielles précédentes.

10. Effectuez l'une des opérations suivantes :

    a. Pour restaurer Data Repository à partir de la dernière sauvegarde, saisissez la commande suivante :

    ```
    /opt/vertica/bin/vbr.py --task restore --config-file
    nom_fichier_chemin_accès_répertoire_configuration
    ```

    nom_fichier_chemin_accès_répertoire_configuration

    Indique le nom de fichier et le chemin d'accès au répertoire du fichier de configuration que vous avez créé lors de l'exécution de la procédure de sauvegarde. Ce fichier se situe à l'emplacement où vous avez exécuté l'utilitaire de sauvegarde (/opt/vertica/bin/vbr.py).

    Par exemple :

    ```
    /opt/vertica/bin/vbr.py --task restore --config-file
    /home/vertica/vert-db-production.ini
    ```

    Remarque : Dans une installation en cluster, vous pouvez exécuter la tâche de restauration à partir de tout hôte inclus dans le cluster.

    b. Pour restaurer Data Repository à partir de l'une des sept sauvegardes incrémentielles précédentes, saisissez la commande suivante :

    ```
    /opt/vertica/bin/vbr.py --task restore --config-file
    nom_fichier_chemin_accès_répertoire_configuration --nom_archive
    ```

    nom_fichier_chemin_accès_répertoire_configuration

    Indique le nom de fichier et le chemin d'accès au répertoire du fichier de configuration à partir duquel vous voulez restaurer une archive. Le fichier de configuration a été créé lorsque vous avez exécuté la procédure de configuration de sauvegarde. Ce fichier se situe à l'emplacement où vous avez exécuté l'utilitaire de sauvegarde (/opt/vertica/bin/vbr.py).

    nom_archive

    Indique le nom du point de restauration spécifique que vous voulez restaurer. Remplacez-le par le répertoire de sauvegarde que le fichier de configuration indique pour le point de restauration. Tous les points de restauration disponibles sont répertoriés. Déterminez le nom de l'archive pour le point de restauration que vous voulez restaurer.

    Par exemple :

    ```
    /opt/vertica/bin/vbr.py --task restore --config-file myconfig.ini --archive
    20131020_170018
    ```

    Remarque : Dans une installation en cluster, vous pouvez exécuter la tâche de restauration à partir de tout hôte inclus dans le cluster.

11. Redémarrez Data Repository en vous connectant à l'ordinateur sur lequel Data Repository est installé en tant qu'administrateur de la base de données *et non* en tant qu'utilisateur root. Ouvrez une invite de commande et procédez comme suit :
    a. Saisissez la commande suivante :

       ```
       /opt/vertica/bin/adminTools
       ```

       La boîte de dialogue Administration Tools s'affiche.
    b. Sélectionnez (3) Démarrer la base de données.
    c. Appuyez sur la barre d'espacement à côté du nom de la base de données, sélectionnez OK et appuyez sur Entrée.

       Vous êtes invité à entrer le mot de passe de la base de données.
    d. Entrez le mot de passe de base de données et appuyez sur Entrée.

       Le Data Repository démarre.
    e. Sélectionnez Exit et appuyez sur Entrée.
12. Redémarrez Data Aggregator en vous connectant à l'ordinateur sur lequel Data Aggregator est installé en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes. Saisissez la commande suivante :

    ```
    /etc/init.d/dadaemon start
    ```

    Data Aggregator démarre.
13. Redémarrez tous les hôtes Data Collector associés au Data Aggregator :
    a. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.
    b. Cliquez sur Data Collectors dans le menu Statut du système.
    c. Sélectionnez tous les hôtes Data Collector qui sont associés à Data Aggregator et cliquez sur Démarrer.

    Les hôtes Data Collector démarrent.

Sauvegarde de Data Aggregator

Dans certains cas, vous devrez sauvegarder Data Aggregator. Par exemple, vous pouvez sauvegarder le Data Aggregator et le Data Repository avant d'effectuer une mise à niveau. Grâce à la sauvegarde de ces composants, vous disposez d'une copie de vos paramètres et de vos certifications personnalisées en cas d'échec inattendu.

Vous ne devez pas arrêter les services du Data Repository, du Data Collector et du Data Aggregator lorsque vous sauvegardez le Data Aggregator.

Les sauvegardes sont stockées à l'emplacement que vous spécifiez, qui peut être sur le système Data Aggregator ou un système hôte de sauvegarde différent.

Remarque : Vous devez avoir des droits root ou sudo pour effectuer cette tâche.

Procédez comme suit :

1. Ouvrez une invite de commande.
2. Utilisez la commande suivante pour créer un répertoire de sauvegarde dans un emplacement sécurisé sur le même système hôte de sauvegarde ou un système différent :

   `mkdir` *`sauvegarde_DA`*

   sauvegarde_DA

   Spécifie le chemin et le nom du répertoire de sauvegarde.
3. Créez des sous-répertoires dans sauvegarde_DA à l'aide de l'ensemble des commandes suivantes :

   ```
   mkdir sauvegarde_DA/deploy_backup
   mkdir sauvegarde_DA/MIBDepot_backup
   mkdir sauvegarde_DA/CustomDeviceType_backup
   ```
4. Exécutez les commandes suivantes pour sauvegarder les fichiers sur DA :
   - Cette commande sauvegarde les certifications de fournisseur personnalisées. Ne sauvegardez pas le fichier local-jms-broker.xml ni les fichiers Readme de ce répertoire.

     ```
     cp répertoire d'installation de Data
     Aggregator/apache-karaf-2.3.0/deploy/im.ca.com.*.xml
     sauvegarde_DA/deploy_backup
     ```
   - Cette commande sauvegarde toutes les MIB personnalisées dans le répertoire MIBDepot :

     ```
     cp répertoire d'installation de Data
     Aggregator/apache-karaf-2.3.0/MIBDepot/* sauvegarde_DA/MIBDepot_backup
     ```
   - Cette commande sauvegarde tous les fichiers XML de sous-type d'unité personnalisés :

     ```
     cp répertoire d'installation de Data
     Aggregator/apache-karaf-2.3.0/custom/devicetype/DeviceType.xml
     sauvegarde_DA/CustomDeviceType_backup/
     ```

   Répertoire d'installation de Data Aggregator

   Spécifie le répertoire d'installation de Data Aggregator.

   Par défaut : /opt/IMDataAggregator.

Restauration de Data Aggregator

Vous pouvez restaurer les informations Data Aggregator que vous avez sauvegardées. Si le Data Repository reste intact, vous pouvez restaurer uniquement le composant Data Aggregator.

La restauration ne requiert pas l'arrêt préalable du Data Aggregator. Les fichiers sauvegardés peuvent être restaurés dans les bons répertoires même lorsque Data Aggregator est en court d'exécution.

Remarque : Vous devez avoir des droits root ou sudo pour effectuer cette tâche.

Procédez comme suit :

1. Ouvrez une invite de commande.
2. (Facultatif) Dans les situations où le service karaf de Data Aggregator n'est pas en cous d'exécution, désinstallez la version de Data Aggregator existante, puis réinstallez-la.
3. Exécutez toutes les commandes suivantes :

   ```
   cp sauvegarde_DA/deploy_backup/*.* répertoire d'installation Data Aggregator/apache-karaf-2.3.0/deploy/
   cp sauvegarde_DA/MIBDepot_backup/*.* répertoire d'installation Data Aggregator/apache-karaf-2.3.0/MIBDepot/
   cp sauvegarde_DA/CustomDeviceType_backup/*.* répertoire d'installation Data Aggregator/apache-karaf-2.3.0/custom/devicetype/
   ```

   Si vous y êtes invité, écrasez le fichier existant.

   sauvegarde_DA

   Spécifie le chemin et le nom du répertoire de sauvegarde.

   Répertoire d'installation de Data Aggregator

   Spécifie le répertoire d'installation de Data Aggregator.

   Par défaut : /opt/IMDataAggregator.
4. Patientez quelques minutes pour que Data Aggregator se synchronise automatiquement avec CA Performance Center. Lorsque les connexions entre Data Aggregator et les hôtes Data Collector sont établies, les hôtes Data Collector recommencent l'interrogation.

   Data Aggregator est restauré.

   Remarque : Si vous devez restaurer un état antérieur de Data Collector, vous pouvez désinstaller, puis réinstaller Data Collector.

Affichage des détails de Data Aggregator

Vous pouvez afficher le nombre d'unités gérables et acceptant la commande ping surveillées par Data Aggregator.

L'administrateur peut afficher le nombre total d'unités gérables et acceptant la commande ping surveillées par Data Aggregator pour tous les clients hébergés. Les totaux des différentes unités pour chaque client hébergé sont également affichés dans un tableau.

Les administrateurs de clients hébergés peuvent afficher le nombre total d'unités gérables et acceptant la commande ping que Data Aggregator surveille pour leur client hébergé.

Vous pouvez également afficher la version et le numéro de compilation de Data Aggregator.

Procédez comme suit :

1. Ouvrez CA Performance Center en tant qu'administrateur.
2. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.
3. Cliquez sur Data Aggregator dans le menu Statut du système.

   La page Liste de Data Aggregator s'ouvre. Le nombre total d'unités gérables et acceptant la commande ping par client hébergé s'affiche, ainsi que la version et le numéro de compilation de l'installation de Data Aggregator sélectionnée.

Affichage de la liste des installations de Data Collector

Vous pouvez afficher une liste des installations de Data Collector disponibles et modifier certains de leurs paramètres. La liste Data Collector indique le client hébergé et le domaine IP auxquels chaque installation de Data Collector est assignée, ainsi que la version et le statut de Data Collector. Vous pouvez également consulter le nombre d'unités et de composants que chaque installation de Data Collector interroge, et le nombre total d'unités assignées à l'instance de Data Collector, y compris celles qui ne sont actuellement pas interrogées.

L'administrateur peut visualiser la liste des installations de Data Collector pour tous les clients hébergés. Les administrateurs de clients hébergés peuvent afficher uniquement les installations de Data Collector qui sont assignées à leur client hébergé.

Procédez comme suit :

1. Ouvrez CA Performance Center en tant qu'administrateur.
2. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.
3. Cliquez sur Data Collectors dans le menu Statut du système.

   La page Liste de Data Collector s'ouvre, affichant une liste des installations de Data Collector.

Informations complémentaires :

Gestion des installations de Data Collector (page 26)

Gestion des installations de Data Collector

L'administrateur doit sélectionner un domaine IP et un client hébergé pour chaque installation de Data Collector. Chaque instance Data Collector peut être associée à un seul domaine IP ; l'instance Data Collector qui est associée à ce domaine IP effectue les demandes de détection.

Les *domaines IP* sont des groupements logiques qui identifient des données provenant d'unités et de réseaux divers. La surveillance par domaine signifie que les adresses IP avec des interfaces ou des applications associées qui appartiennent à différents réseaux de clients sont surveillées séparément. Lorsqu'ils sont combinés avec des autorisations appropriées, les domaines IP sont surveillés à partir d'une console unique, mais les utilisateurs affichent seulement les données qui concernent les domaines qu'ils surveillent.

Un *client hébergé* représente un environnement de client qu'un fournisseur de services gérés administre. Chaque environnement de client hébergé est indépendant et fonctionne en tant qu'instance distincte de CA Performance Center. Chaque instance peut contenir plusieurs utilisateurs et des rôles qui ne sont pas partagés entre les clients hébergés.

Le client hébergé par défaut représente l'espace de client hébergé pour le fournisseur de services gérés dans l'infrastructure gérée. Affectez le client hébergé par défaut si vous ne déployez pas l'hébergement multiclient. Dans un environnement de client hébergé unique, le client hébergé par défaut est l'espace utilisé pour surveiller l'intégralité de l'infrastructure.

Procédez comme suit :

1. Ouvrez CA Performance Center en tant qu'administrateur.
2. Accédez à la page Data Collectors (page 25).
3. Sélectionnez une instance Data Collector dans la liste.
4. Vérifiez que le composant Data Collector est disponible pour affectation. La colonne Eléments interrogés catalogue le nombre d'unités interrogées et les composants affectés à cette instance de Data Collector.

   Important : Si vous interrogez plusieurs unités et composants, vous ne pouvez pas modifier le client hébergé ou le domaine IP affecté à une instance Data Collector.
5. Cliquez sur Assigner.

   La boîte de dialogue Assigner un Data Collector s'ouvre.
6. Dans la liste déroulante, sélectionnez le client hébergé que vous souhaitez assigner à cette instance Data Collector.

   Toutes les unités et tous les composants détectés par cette instance Data Collector sont automatiquement associés à ce client hébergé.

   Si vous voulez utiliser le client hébergé par défaut, sélectionnez Client hébergé par défaut.
7. Sélectionnez le domaine IP que vous souhaitez associer à cette instance Data Collector.

   Toutes les unités et tous les composants gérés détectés par cette instance Data Collector sont automatiquement associés à ce domaine IP.
8. Cliquez sur Enregistrer.

   Le client hébergé et le domaine IP sont affectés à l'installation de Data Collector.

Rééquilibrage de la charge sur Data Collector

Lorsqu'une instance de Data Collector surveille un grand nombre d'unités, un dépassement de la capacité et une surcharge peuvent se produire. Vous pouvez transférer la charge de travail d'une instance de Data Collector surchargée à d'autres instances de Data Collector. Vous pouvez rééquilibrer la charge sur Data Collector de deux façons :

- Sélectionnez l'instance de Data Collector surchargée, puis sélectionnez l'option Rééquilibrer. La charge est automatiquement rééquilibrée sur d'autres instances de Data Collector disponibles.
- Déplacez les unités sélectionnées d'une instance de Data Collector à une autre.

Important : Il est recommandé de ne pas rééquilibrer la charge sur le Data Collector et de ne pas déplacer un grand nombre d'éléments d'une instance du Data Collector vers une autre pendant les heures de pics d'activités étant donné que cela peut avoir une incidence sur les performances des utilisateurs finaux.

Procédez comme suit :

1. Ouvrez CA Performance Center en tant qu'administrateur.
2. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.
3. Cliquez sur Data Collectors dans le menu Statut du système.

   Vous pouvez afficher le nombre d'unités et de composants que chaque installation de Data Collector interroge. Vous pouvez également consulter le nombre total d'unités assignées à chaque instance de Data Collector, y compris les unités qui ne sont actuellement pas interrogées.

Rééquilibrage automatique de la charge sur Data Collector

1. Sélectionnez les instances de Data Collector que vous voulez rééquilibrer et cliquez sur Rééquilibrer.

   Remarque : Sélectionnez des instances de Data Collector qui appartiennent au même domaine IP. Seules les instances de Data Collector d'un même domaine IP permettent de rééquilibrer la charge des unités.
2. Une boîte de dialogue de confirmation affiche l'unité actuelle et le nombre d'éléments interrogés pour chaque instance de Data Collector sélectionnée, ainsi que l'unité proposée et le nombre d'éléments interrogés après le rééquilibrage.

   Remarque : Vous pouvez uniquement déplacer des unités vers des instances de Data Collector qui peuvent les contacter.

3. Cliquez sur Yes (Oui).

   Remarque : Le rééquilibrage d'éléments interrogés redémarre les calculs de moyenne de référence pour tous les éléments interrogés rééquilibrés.

Déplacement d'unités sélectionnées vers une instance de Data Collector

1. Sélectionnez l'instance de Data Collector à partir de laquelle vous voulez déplacer les unités sélectionnées.
2. Dans la table Unités, sélectionnez les unités à déplacer vers une autre instance de Data Collector, puis cliquez sur Déplacer les unités.
3. La boîte de dialogue Déplacer les unités vers le Data Collector sélectionné s'ouvre.
4. Dans la liste déroulante, sélectionnez l'instance de Data Collector vers laquelle vous voulez déplacer les unités sélectionnées.

   Remarque : Seules les instances de Data Collector appartenant au même domaine IP peuvent être sélectionnées.
5. Cliquez sur Yes (Oui).

   Remarque : Le déplacement d'unités redémarre les calculs de moyenne de référence pour les unités déplacées.

Equilibrage de la charge pour des Data Collector qui extraient des données non-SNMP (CAMM)

L'équilibrage de la charge du Data Collector par le déplacement d'unités et de composants d'une instance du Data Collector vers une autre ne s'applique qu'à des unités et à des composants surveillés via SNMP ou ICMP. Dans le cas d'instances du Data Collector qui extraient des données non-SNMP via CAMM et qui exigent un rééquilibrage des ressources, vous pouvez effectuer l'opération en distribuant les moteurs de pack d'unités sur d'autres hôtes de l'environnement. Voici les instructions pour effectuer ce rééquilibrage.

1. Installez un contrôleur local (LC) sur le nouveau serveur et pointez sur le serveur MC (Multi Controller, contrôleur multiple) approprié pendant l'installation
2. Une fois le LC installé sur le nouveau serveur, vérifiez que CAMM présente deux LC.
   a. Ouvrez CAMMWEB.
   b. Cliquez sur Hôtes. Le LC installé (nouveau serveur) devrait être visible.
3. A l'aide de CAMMWEB, sélectionnez le nouveau serveur et déployez les moteurs de pack d'unités à migrer.
4. Connectez-vous au serveur MC et accédez à :

   Répertoire
   $CAMM_INSTALL/MC/repository/<IP_ANCIEN_SERVEUR>/COMPONENTS

5. Exécutez la commande suivante :

   'cp –R ENGINE_<pack_unités> $CAMM_INSTALL/MC/repository/<IP_NOUVEAU_SERVEUR>/COMPONENTS/'

6. Si le pack d'unités à migrer utilise le mécanisme sftp/FTP/copie pour la collecte de données,

   a. créez les répertoires suivants sous $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<pack_unités>/ sur NOUVEAU_SERVEUR.

      - répertoire tmp sous $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<pack_unités>/tmp/input/inventory
      - répertoire d'entrée sous $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<pack_unités>/tmp/input/performance

   b. Copiez les fichiers suivants de ANCIEN_SERVEUR vers NOUVEAU_SERVEUR.

      - $CAMM_INSTALL/COMPONENTS/ENGINE_<pack_unités>/tmp/input/inventory/.historyFile.Inventory vers $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<pack_unités>/tmp/input/inventory.
      - $CAMM_INSTALL/COMPONENTS/ENGINE_<pack_unités>/tmp/input/performance/.historyFile.Performance to $CAMM_INSTALL/LC/repository/COMPONENTS/ENGINE_<pack_unités>/tmp/input/performance

7. Démarrez le pack d'unités à partir de CAMMWEB.

Procédure de déplacement de Data Collector vers un autre hôte

Data Collector est un composant de Data Aggregator. Vous pouvez déplacer Data Collector vers un autre système hôte sans devoir redétecter les unités et composants du réseau ni perdre de données historiques. Par exemple, si vous êtes un administrateur d'outils, votre administrateur de serveur peut vous charger de déplacer Data Collector vers un autre hôte. Data Collector interroge 500 000 unités et composants. Il est donc important de ne pas perdre de données et de ne pas avoir à effectuer de nouvelle détection.

Vous pouvez déplacer le composant Data Collector même si les packs d'unités sont installés.

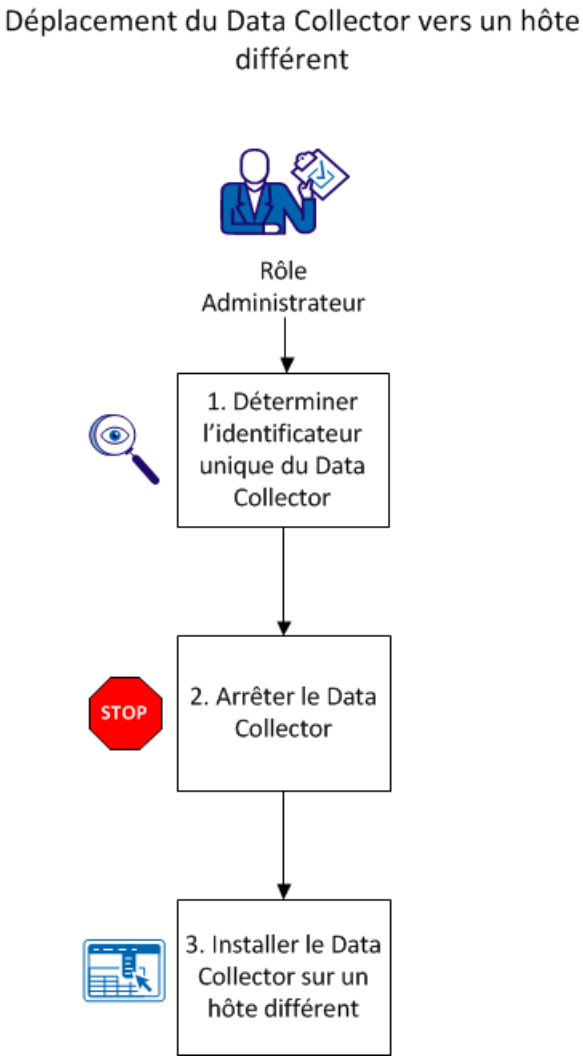
Tenez compte des remarques suivantes :

- La quantité de perte de données correspond à la durée écoulée entre la fermeture de l'ancien composant Data Collector et le déploiement du nouveau composant Data Collector.
- Si l'ancien composant Data Collector démarre accidentellement, l'interrogation des données SNMP est doublée. Un avertissement similaire à l'avertissement suivant s'affiche dans le journal karaf de Data Aggregator :

  ```
  WARN  | Session Task-810 | 2013-01-02 13:52:09,062 | DCHeartBeatLog |
  ore.collector.interfaces |
        | HeartBeat message not received (message de signal d'activité non reçu)
  Attendus : 93, reçus : 255
  ```

  Pour corriger ce problème, arrêtez ou désinstallez l'ancien composant Data Collector.

Le diagramme suivant affiche la procédure à suivre pour déplacer Data Collector vers un hôte différent :



Pour déplacer Data Collector vers un autre système, suivez ce processus :

1. Déterminez l'identificateur unique pour le Data Collector (page 33).
2. Arrêtez Data Collector (page 33).
3. (Pour l'intégration de CA Mediation Manager uniquement) Migrez les packs d'unités (page 35).
4. Installez Data Collector sur un autre hôte (page 35).

Déterminez l'identificateur unique pour Data Collector.

Déterminez l'identificateur unique pour Data Collector avant de déplacer ce composant vers un autre hôte.

Récupérez l'ID de Data Collector en suivant *une* des méthodes suivantes :

- Connectez-vous à CA Performance Center en tant qu'utilisateur avec le rôle Administrateur et suivez les étapes suivantes :
  a. Sélectionnez Administration, puis sélectionnez une source de données Data Aggregator dans le menu.
  b. L'interface d'administration de Data Aggregator s'ouvre.
  c. Sélectionnez Statut du système, Data Collectors dans le menu.
  d. Recherchez le composant Data Collector que vous voulez déplacer et notez son ID.
- Ouvrez un navigateur Web et publiez l'appel de service Web suivant :

  `http://DA_hostname:port/rest/dcms`

  DA_hostname:port

  Spécifie le nom d'hôte de Data Aggregator et le numéro de port.

  Port par défaut : 8581

  Recherchez la section <DataCollectionMgrInfo> où les paramètres HostName et IPAddress correspondent à celui que vous voulez déplacer. Notez la valeur de <DcmID>.

Ensuite, arrêtez les services Data Collector sur l'hôte actuel.

Arrêtez Data Collector.

Arrêtez les services Data Collector sur l'hôte actuel avant de déplacer Data Collector vers un autre hôte.

Procédez comme suit :

1. Si vous avez installé des packs d'unités pour ce Data Collector, procédez comme suit : Si aucun pack d'unités n'a été installé, allez à l'étape 2.
   a. Connectez-vous à CA Performance Center en tant qu'utilisateur avec le rôle d'administrateur.
   b. Sélectionnez Administration, puis sélectionnez une source de données Data Aggregator dans le menu.

      L'interface d'administration de Data Aggregator s'ouvre.
   c. Allez dans le menu Configuration de la surveillance et sélectionnez Profils d'intégration d'EMS.
   d. Cliquez avec le bouton droit de la souris sur un profil associé à cet hôte Data Collector et sélectionnez Arrêter. Suivez cette étape pour tous les profils EMS liés à cet hôte Data Collector.
   e. Archivez les artefacts CA Mediation Manager en exécutant la commande suivante :

      `tar -zcvf` *`nom de fichier`*
      `/opt/IMDataCollector/apache-karaf-{n.n.n}/MediationCenter`

      Nom de fichier

      Spécifie le nom du fichier d'archivage.

      Remarque : Ce fichier d'archive est déplacé vers le nouvel hôte Data Collector ultérieurement.
2. Connectez-vous à l'hôte Data Collector et exécutez la commande suivante :

   `/etc/init.d/dcmd stop`
3. Vérifiez que le Data Collector est arrêté :
   a. Connectez-vous à CA Performance Center en tant qu'utilisateur avec le rôle d'administrateur.
   b. Sélectionnez Administration, puis sélectionnez une source de données Data Aggregator dans le menu.
   c. Sélectionnez Statut du système, Data Collectors dans le menu.
   d. Vérifiez que Data Collector affiche le statut Non connecté.

Ensuite, installez Data Collector sur le nouvel hôte.

Installation de Data Collector sur un autre hôte

Après avoir arrêté les services Data Collector sur l'ancien hôte, installez Data Collector sur un nouvel hôte. Les données de Data Collector sur l'ancien hôte sont exportées vers le nouvel hôte lors de cette procédure.

Procédez comme suit :

1. (Pour l'intégration à CA Mediation Manager uniquement) Migrez vos packs d'unités. Dans l'ancien hôte Data Collector, exécutez le script *$CAMM_HOME*/tools/migratePMtoCAMM avec l'indicateur -t.

   Cette étape suppose que vous exécutez le script sur un serveur Data Collector équipé d'un contrôleur local. Vous devez également avoir exécuté de la console CA Mediation Manager sur un autre serveur.

   Remarque : Les packs d'unités migrés sont copiés dans le répertoire *$CAMM_HOME*/MigratedIMDevicepacks sous forme de fichiers ZIP. Pour plus d'informations sur la migration des packs d'unités, consultez le scénario Procédure de migration des packs d'unités.

2. Connectez-vous au nouveau système hôte et ouvrez une session d'interface de commande.

3. Définissez une variable d'environnement avec l'ID que vous avez copié préalablement en exécutant cette commande :

   `export DCM_ID=`*`ID du Data Collector`*

4. Dans la même session, exécutez le fichier binaire **install.bin** pour installer le Data Collector.

5. Installez CA Mediation Manager LC sur le même serveur.

6. Si vous avez préalablement installé des packs d'unités pour ce Data Collector, effectuez ces étapes supplémentaires :

   a. Copiez les fichiers ZIP que vous avez créés préalablement à l'aide du script de migration dans des répertoires locaux sur cet hôte.

   b. A l'aide de la console Web CA Mediation Manager, déployez ces packs d'unités et démarrez-les.

      Remarque : Vous *n'avez pas besoin* de redéployer les packs de certification sur l'hôte Data Aggregator.

Remarque : Après quelques cycles d'interrogation, vérifiez que les données sont collectées par le nouvel hôte Data Collector.

Nous vous recommandons de désinstaller l'ancien Data Collector et de supprimer les profils d'EMS associés après avoir vérifié que les données sont collectées sur le nouvel hôte. Il s'agit d'une bonne pratique, cette étape n'est pas requise.

La présente Documentation, qui inclut des systèmes d'aide et du matériel distribués électroniquement (ci-après nommés "Documentation"), vous est uniquement fournie à titre informatif et peut être à tout moment modifiée ou retirée par CA. La présente Documentation est la propriété exclusive de CA et ne peut être copiée, transférée, reproduite, divulguée, modifiée ou dupliquée, en tout ou partie, sans autorisation préalable et écrite de CA.

Si vous êtes titulaire de la licence du ou des produits logiciels décrits dans la Documentation, vous pourrez imprimer ou mettre à disposition un nombre raisonnable de copies de la Documentation relative à ces logiciels pour une utilisation interne par vous-même et par vos employés, à condition que les mentions et légendes de copyright de CA figurent sur chaque copie.

Le droit de réaliser ou de mettre à disposition des copies de la Documentation est limité à la période pendant laquelle la licence applicable du logiciel demeure pleinement effective. Dans l'hypothèse où le contrat de licence prendrait fin, pour quelque raison que ce soit, vous devrez renvoyer à CA les copies effectuées ou certifier par écrit que toutes les copies partielles ou complètes de la Documentation ont été retournées à CA ou qu'elles ont bien été détruites.

DANS LES LIMITES PERMISES PAR LA LOI APPLICABLE, CA FOURNIT LA PRÉSENTE DOCUMENTATION "TELLE QUELLE", SANS AUCUNE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT CONCERNANT LA QUALITÉ MARCHANDE, L'ADÉQUATION À UN USAGE PARTICULIER, OU DE NON-INFRACTION. EN AUCUN CAS, CA NE POURRA ÊTRE TENU POUR RESPONSABLE EN CAS DE PERTE OU DE DOMMAGE, DIRECT OU INDIRECT, SUBI PAR L'UTILISATEUR FINAL OU PAR UN TIERS, ET RÉSULTANT DE L'UTILISATION DE CETTE DOCUMENTATION, NOTAMMENT TOUTE PERTE DE PROFITS OU D'INVESTISSEMENTS, INTERRUPTION D'ACTIVITÉ, PERTE DE DONNÉES OU DE CLIENTS, ET CE MÊME DANS L'HYPOTHÈSE OÙ CA AURAIT ÉTÉ EXPRESSÉMENT INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES OU PERTES.

L'utilisation de tout produit logiciel mentionné dans la Documentation est régie par le contrat de licence applicable, ce dernier n'étant en aucun cas modifié par les termes de la présente.

CA est le fabricant de la présente Documentation.

Le présent Système étant édité par une société américaine, vous êtes tenu de vous conformer aux lois en vigueur du Gouvernement des Etats-Unis et de la République française sur le contrôle des exportations des biens à double usage et aux autres réglementations applicables et ne pouvez pas exporter ou réexporter la documentation en violation de ces lois ou de toute autre réglementation éventuellement applicable au sein de l'Union Européenne.

Copyright © 2014 CA. Tous droits réservés. Tous les noms et marques déposées, dénominations commerciales, ainsi que tous les logos référencés dans le présent document demeurent la propriété de leurs détenteurs respectifs.

Changements de configuration de Data Aggregator en cas de déconnection réseau d'un hôte Data Collector

Occasionnellement, la connexion entre un hôte Data Aggregator et un hôte Data Collector est rompue, par exemple, en cas de déconnexion réseau. Si les processus de Data Aggregator et de Data Collector sont en cours d'exécution lorsque survient une déconnexion, vous pouvez apporter des changements de configuration à l'installation de Data Aggregator. Dans ce cas, l'interrogation se poursuit sur l'hôte Data Collector en fonction de la configuration qui existait avant la déconnexion réseau. Une fois que la connexion entre les hôtes Data Aggregator et Data Collector est rétablie, Data Collector télécharge la nouvelle configuration et ajuste l'interrogation en conséquence.

Par exemple, vous faites l'une des modifications de configuration suivantes :

- Vous changez l'expression qu'une certification de fournisseur SNMP utilise pour calculer une valeur sur une famille de mesures.
- Changement de la famille de mesures pour interroger une nouvelle mesure opérationnelle.

Lorsque la connexion entre les hôtes Data Aggregator et Data Collector est rompue, les modifications ne peuvent pas prendre effet. Après le rétablissement de la connexion, Data Collector commence à interroger les nouveaux objets MIB SNMP utilisés dans la nouvelle expression ou dans le calcul de la nouvelle mesure opérationnelle.

Mise en cache Data Collector des données interrogées lorsque l'hôte Data Aggregator est indisponible

Occasionnellement, la connexion au réseau entre les hôtes Data Aggregator et Data Collector est interrompue. Dans ce cas, Data Collector poursuit l'interrogation et met en cache les données d'interrogation dans la mémoire, jusqu'à une limite configurable. Lorsque l'hôte Data Aggregator redevient disponible, les données interrogées mises en cache sont envoyées à Data Aggregator.

Les données d'interrogation sont traitées au fil de leur arrivée. En d'autres termes, les données d'interrogation mises en cache les plus anciennes sont envoyées à Data Aggregator en premier. Si la limite de mémoire du cache est atteinte, les nouvelles données d'interrogation sont enregistrées uniquement lorsque l'hôte Data Aggregator devient disponible et après le traitement de 9 % des données mises en cache par cet hôte.

Important : L'utilisation de la mémoire augmente considérablement sur le système Data Collector lorsque Data Aggregator n'est pas disponible.

La quantité d'espace de stockage requis au niveau de la mémoire peut varier et dépend des facteurs suivants :

- Nombre d'unités et de composants interrogés
- Taux d'interrogation
- Quantité de données que vous souhaitez conserver lorsque l'hôte Data Aggregator n'est pas disponible

La valeur par défaut de la limite de mémoire du cache correspond à la moitié de la mémoire maximum de processus de Data Collector. Vous avez configuré l'utilisation de la mémoire maximum lorsque vous avez installé Data Collector ou ultérieurement à l'installation.

Data Collector requiert une quantité dédiée de mémoire pour fonctionner correctement. Dans un environnement de taille réduite où Data Collector interroge 50 000 unités et composants à un intervalle d'interrogation défini sur cinq minutes, 2 Go de mémoire sont requis pour un fonctionnement minimum. Dans un environnement de grande taille où Data Collector interroge 500 000 unités et composants à un intervalle d'interrogation défini sur cinq minutes, 24 Go de mémoire sont requis pour un fonctionnement minimum. Vous pouvez utiliser la mémoire restante pour mettre en cache les données d'interrogation.

Calcul de la mémoire requise pour la mise en cache des données d'interrogation

La quantité de mémoire requise pour la mise en cache des données interrogées varie selon les éléments suivants :

- Echelle de votre environnement
- Durée de stockage des données lorsque l'hôte Data Aggregator n'est pas disponible

Utilisez la formule suivante pour calculer la quantité de mémoire requise pour la mise en cache des données :

```
Cache requis (Go) = (durée de mise en cache des données (secondes)×nombre d'éléments interrogés)/(262144×taux moyen d'interrogation (secondes))
```

Exemple : calcul de la mémoire requise pour la mise en cache des données interrogées pendant une heure

- Calculez la mémoire requise dans un environnement à petite échelle où Data Collector interroge 50 000 unités et composants à un intervalle d'interrogation de cinq minutes. Vous souhaitez mettre en cache les données interrogées pendant une heure lorsque le Data Aggregator n'est pas disponible :

  Cache requis (Go)=(3600 ×50000)/(262144 ×300)

  Cache requis (Go)=2,3 Go

  Remarque : Ce calcul se fait en plus de la mémoire opérationnelle de base requise. Un environnement à petite échelle requiert une mémoire opérationnelle de base de 2 Go. La mémoire totale requise est donc de 4608 Mo (2 Go + 2,3 Go).

- Calculez la mémoire requise dans un environnement à grande échelle où Data Collector interroge 500 000 unités et composants à un intervalle d'interrogation de cinq minutes. Vous souhaitez mettre en cache les données interrogées pendant une heure lorsque le Data Aggregator n'est pas disponible :

  Cache requis (Go)=(3600 ×500000)/(262144 ×300)

  Cache requis (Go)=22,9 Go

  Remarque : Ce calcul se fait en plus de la mémoire opérationnelle de base requise. Un environnement à grande échelle requiert une mémoire opérationnelle de base de 24 Go. La mémoire totale requise est donc de 47 Go (24 Go + 22,9 Go).

Modification de la limite de mémoire du cache de données

Vous pouvez modifier la quantité de données que ce Data Collector doit mettre en cache lorsque le composant Data Aggregator cesse d'être disponible.

Procédez comme suit :

1. Calculez la quantité de mémoire requise pour la mise en cache des données (page 38).
2. Notez la quantité de mémoire requise pour la mise en cache des données.
3. Connectez-vous au serveur sur lequel Data Collector est installé. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

   Remarque : Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator.*
4. Arrêtez Data Collector à l'aide de cette commande :

   ```
   service dcmd stop
   ```

5. Modifiez la valeur de la mémoire IM_MAX_MEM pour Data Collector :
   a. Ouvrez le fichier *répertoire d'installation de Data Collector*/apache-karaf-2.3.0/jms/local-jms-broker.xml.
   b. Définissez la valeur de la limite IM_MAX_MEM sur le double de la valeur que vous avez notée dans cette étape. 2.Vérifiez que cette valeur ne dépasse pas la mémoire RAM disponible sur le système.
6. Modifiez la limite de mémoire du cache du courtier JMS sur Data Collector :
   a. Ouvrez le fichier *répertoire d'installation de Data Collector*/apache-karaf-2.3.0/jms/local-jms-broker.xml.
   b. Localisez la ligne suivante :

      ```
      <memoryUsage limit="value"/>
      ```

      value

      Correspond à la limite actuelle du cache.
   c. Remplacez la valeur actuelle de la limite du cache par celle que vous avez calculée préalablement et enregistrez le fichier.
7. Indiquez à Data Collector les modifications apportées au fichier jms/local-jms-broker.xml. Saisissez la commande suivante pour déployer un faux fichier .lock. Un faux fichier .lock indique à Data Collector qu'un arrêt non approprié a eu lieu :

   ```
   echo `date` > /opt/IMDataCollector/apache-karaf-2.3,0/.lock
   ```
8. Redémarrez Data Collector à l'aide de cette commande :

   ```
   service dcmd start
   ```

   La limite de la mémoire du cache est configurée.

Processus d'audit du Data Repository

Le processus d'audit réalise un audit quotidien de la base de données à 03 h 00, pour calculer l'espace total que les données Data Aggregator occupent. Il estime la taille de la base de données à l'aide de la fonction audit de Vertica. L'estimation de la taille de la base de données n'inclut pas les données stockées dans les tables temporaires, les données qui ont été marquées comment devant être supprimées mais qui ne sont pas purgées dans la base de données, ni les données incluses dans les tables de surveillance Vertica.

CA Technologies a signé un contrat de licence avec Vertica stipulant que le total des données stockées dans le Data Repository ne peut pas dépasser 32 To.

Pour afficher le résultat le plus récent d'un audit, accédez à l'URL suivante dans votre navigateur :

http://*nom_hôte:port*/rest/datarepositorymaintenance/audit

Cette URL renvoie un fichier XML. La balise Current Size (Taille actuelle) indique la taille actuelle du Data Repository en octets.

Important : Révisez les résultats d'audit à intervalles réguliers. Une valeur supérieure à 32 To n'est pas conforme au contrat de licence. Contactez le service de support technique d'Oracle si vous avez besoin d'une aide supplémentaire.

Processus de surveillance du signal d'activité de Data Repository

Le processus de surveillance du signal d'activité vérifie si le Data Repository est en cours d'exécution toutes les 10 secondes. Si ce processus ne parvient pas à confirmer que la base de données sera activée dans 5 minutes, Data Aggregator se ferme. Un message d'audit est journalisé dans le fichier *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/shutdown.log.

Dans un environnement de cluster, un processus vérifie, toutes les 10 secondes, que les noeuds du cluster sont disponibles. Si vous ne parvenez pas à contacter un noeud dans un délai de 5 minutes, un événement est généré et journalisé au niveau de l'unité Data Aggregator dans CA Performance Center. Un message d'audit est journalisé dans le fichier *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/shutdown.log.

Si le noeud du Data Repository injoignable est le noeud principal (utilisé pour toutes les requêtes du Data Aggregator), le Data Aggregator bascule automatiquement vers le noeud de Data Repository disponible suivant. Un événement est généré et journalisé au niveau de l'unité Data Aggregator.

Important : Certaines fonctions administratives qui ont lieu pendant un basculement de haute disponibilité sont interrompues, puis échouent. Un cycle d'interrogation est alors perdu. Ces fonctions ne reprendront pas une fois le Data Repository connecté à un autre noeud dans l'environnement de cluster. Les fonctions d'administration que vous effectuez une fois le Data Repository connecté à un autre noeud dans l'environnement de cluster fonctionnent comme prévu.

Le Data Aggregator s'arrête lorsque tous les noeuds du Data Repository sont impossibles à contacter dans un environnement de cluster.

La perte de contact avec le Data Repository peut aboutir à une perte de données par le Data Aggregator. Résolvez tout problème de connectivité ou lié au Data Repository avant de redémarrer le Data Aggregator. Le Data Aggregator se ferme automatiquement s'il ne parvient pas à se connecter au Data Repository au démarrage. Pour limiter la perte de données, les installations Data Collector continuent de collecter et de stocker des données localement pendant un certain temps jusqu'à ce que Data Aggregator soit redémarré.

Sélectionnez l'option Restart Vertica on Host dans le menu principal de l'utilitaire admintools et suivez les invites. Data Aggregator n'établira un signal d'activité sur le noeud ayant échoué qu'après le redémarrage du processus Vertica sur ce noeud et l'établissement d'une connexion au réseau.

Choix d'autre hôte dans un cluster en cas de panne de l'hôte sélectionné

Si l'hôte de base de données qui est spécifié pendant l'installation de Data Aggregator échoue à l'exécution, Data Aggregator s'arrête automatiquement. Si vous avez installé le Data Repository dans un cluster, faites pointer les connexions de la base de données vers un autre hôte dans le cluster avant de redémarrer le Data Aggregator.

Procédez comme suit :

1. Ouvrez le fichier *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/etc/dbconnection.cfg sur l'hôte Data Aggregator.
2. Modifiez la ligne suivante dans le fichier dbconnection.cfg. Modifiez cette ligne pour référencer un nom d'hôte ou une adresse IP d'un des hôtes de cluster du Data Repository qui est toujours actif :

   `dbUrl=jdbc:vertica://`*`nom d'hôte du serveur de base de données`*`:`*`port du serveur des base de données`*`/databasename?use35CopyFormat=true&BinaryDataTransfer=false`

   nom_hôte_serveur_base_données* : *port_serveur_base_données

   Indique le nom d'hôte ou l'adresse IP ainsi que le numéro de port du Data Repository que vous avez spécifiés lors de l'installation du Data Aggregator.

   Numéro de port par défaut : 5433

   Exemple :

   Si host2 est en cours d'exécution dans le cluster et que vous choisissez de pointer les connexions de la base de données vers host2, votre entrée dbUrl mise à jour peut se présenter comme suit :

   ```
   dbUrl=jdbc:vertica://host2:5433/mydatabasename?use35CopyFormat=true&BinaryDataTransfer=false
   ```

3. Enregistrez le fichier dbconnection.cfg.

4. Pour redémarrer Data Aggregator, saisissez la commande suivante :

   ```
   /etc/init.d/dadaemon start
   ```

5. Pour garantir que Data Aggregator n'est plus en cours d'exécution, saisissez la commande suivante :

   ```
   Ps –ef | grep java | grep –v grep
   ```

   Les processus Data Aggregator ne sont pas renvoyés si Data Aggregator ne s'exécute pas.

   Les connexions à la base de données pointent désormais vers l'hôte spécifié dans le cluster.

Si plusieurs hôtes du cluster Data Repository sont injoignables, le Data Repository et le Data Aggregator se ferment automatiquement. Le cluster du Data Repository peut perdre uniquement un hôte.

Data Aggregator se ferme lorsqu'un hôte unique appartenant au cluster et qui n'est *pas* spécifié pendant l'installation de Data Aggregator se déconnecte du réseau (par exemple, suite à l'activation d'un pare-feu ou au retrait du câble Ethernet). Data Aggregator redémarre automatiquement si vous activé la récupération automatique du processus Data Aggregator pendant l'installation de Data Aggregator. Une fois que l'hôte qui est hors ligne devient disponible, renvoyez cet hôte au cluster. Sélectionnez l'option Restart Vertica on Host dans le menu principal de l'utilitaire admintools et suivez les invites.

Remarque : Pour plus d'informations sur la configuration de la récupération automatique du processus Data Aggregator, consultez le Manuel d'installation de *Data Aggregator*.

Si un hôte unique appartenant au cluster et qui n'est *pas* spécifié pendant l'installation de Data Aggregator est arrêté à l'aide de l'option Kill Vertica Process on Host (du menu Avancé de l'utilitaire admintools), Data Aggregator continue de fonctionner. Une fois que l'hôte qui est hors ligne devient disponible, renvoyez cet hôte au cluster. Sélectionnez l'option Restart Vertica on Host dans le menu principal de l'utilitaire admintools et suivez les invites.

Modification l'utilisation maximum de la mémoire pour les composants Data Aggregator et Data Collector après l'installation (facultatif)

La valeur de l'utilisation maximum par défaut de la mémoire des composants Data Aggregator et Data Collector n'est pas suffisante. Pour une exécution efficace dans un déploiement à grande-échelle, modifiez l'utilisation de la mémoire maximum pour Data Aggregator et Data Collector. Cette modification est possible pendant ou après l'installation. Par défaut, l'utilisation de la mémoire pour Data Aggregator et Data Collector est de 2 Go.

Important : Dans cette procédure, les modifications de mémoire sont appliquées dans un contexte où Data Aggregator et Data Collector sont installés sur des ordinateurs distincts. Cette procédure suppose également que ces ordinateurs soient dédiés uniquement à l'installation de ces composants.

Procédez comme suit :

1. Ouvrez une console et entrez la commande suivante :

   ```
   more /proc/meminfo
   ```

   L'utilisation totale de la mémoire est affichée.

2. Notez cette mémoire totale.

3. Modifiez la mémoire maximum pour Data Aggregator en effectuant les étapes suivantes :

   a. Accédez au fichier *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/bin/setenv.

   b. Modifiez la ligne IM_MAX_MEM=*nombre unité* pour les déploiements volumineux.

      nombre unité

      Indique la quantité maximale de mémoire. Le *nombre* correspond à un nombre entier positif et l'*unité* est G (giga) ou M (méga). Déduisez 2 Go de la mémoire totale que vous avez notée préalablement et entrez la valeur ici. 2 Go sont réservés pour d'autres opérations au niveau du système d'exploitation.

      Exemple : 33544320 Ko - 2o = 30 Go

      IM_MAX_MEM=30G

      Par exemple :

      IM_MAX_MEM=4G

   c. Enregistrez le fichier.

d. Redémarrez Data Aggregator à l'aide de la commande suivante :

```
service dadaemon start
```

Data Aggregator démarre et se synchronise automatiquement avec CA Performance Center.

e. Afin de conserver la modification du paramètre de mémoire lors d'une mise à niveau de Data Aggregator, modifiez le fichier /etc/DA.cfg en remplaçant la valeur mise à jour par la propriété da.memory.

Par exemple :

```
da.memory=4G
```

4. Modifiez la mémoire maximum pour tous les hôtes Data Collector en effectuant les étapes suivantes :

a. Accédez au fichier *répertoire d'installation de Data Collector*/apache-karaf-2.3.0/bin/setenv.

b. Modifiez la ligne IM_MAX_MEM=*nombre unité* pour les déploiements volumineux.

nombre unité

Indique la quantité maximale de mémoire. Le *nombre* correspond à un nombre entier positif et l'*unité* est G (giga) ou M (méga). Déduisez 2 Go de la mémoire totale que vous avez notée préalablement et entrez la valeur ici. 2 Go sont réservés pour d'autres opérations au niveau du système d'exploitation.

Exemple : 33544320 Ko - 2o = 30 Go

IM_MAX_MEM=30G

Par exemple :

IM_MAX_MEM=4G

c. Enregistrez le fichier.

d. Redémarrez les hôtes Data Collector à l'aide de la commande suivante :

```
service dcmd start
```

e. Afin de conserver la modification du paramètre de mémoire lors d'une mise à niveau de Data Collector, modifiez le fichier /opt/DCM.cfg en remplaçant la valeur mise à jour par la propriété IM_MAX_MEM.

Par exemple :

```
IM_MAX_MEM=4G
```

La quantité maximale de mémoire est configurée pour des déploiements volumineux.

Exemple : Configurez l'utilisation de la mémoire maximum pour Data Aggregator après avoir installé Data Aggregator

L'exemple suivant configure l'utilisation de la mémoire maximum pour Data Aggregator où la mémoire totale est de 3354432 Ko :

1. Ouvrez une console et entrez la commande suivante :

   ```
   more /proc/meminfo
   ```

   Les résultats suivants s'affichent :

   ```
   MemTotal : 33554432KB
   ```

2. Calculez la mémoire maximale requise pour les déploiements volumineux :

   Equation : mémoire totale - 2 G = mémoire maximum pour les déploiements à grande échelle

   Solution : 3354432 KB - 2G = 30G

3. Accédez au fichier *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/bin/setenv.

4. Modifiez la ligne IM_MAX_MEM=*nombre unité* pour les déploiements volumineux :

   IM_MAX_MEM=30G

5. Enregistrez le fichier.

6. Redémarrez Data Aggregator.

   La quantité maximale de mémoire est modifiée pour les déploiements volumineux.

Modification de la limite de mémoire externe d'ActiveMQ après l'installation (facultatif)

Le programme d'installation de Data Aggregator calcule la mémoire du système nécessaire au processus ActiveMQ. Toutefois, vous pouvez modifier manuellement les paramètres de limite de mémoire pour ajuster ActiveMQ à votre système Data Aggregator. Par exemple, vous pouvez modifier les paramètres dans les circonstances suivantes :

- Lorsque la mémoire du système a été modifiée.
- Lorsque le nombre de systèmes Data Collector a été modifié.
- Pour optimiser les paramètres de mémoire.
- Lorsque vous avez déterminé à l'aide de la console JConsole ou du graphique personnalisé de CA Infrastructure Management avec les mesures d'ActiveMQ, que les performances d'ActiveMQ se sont détériorées.

Procédez comme suit :

1. Calculez la quantité de mémoire pour ActiveMQ selon les paramètres suivants :

   Taille maximum du segment de mémoire Java

   Cette valeur est définie par défaut sur 20 % de la mémoire du système. La valeur minimum est 512 Mo.

   Taille minimum initiale du segment de mémoire Java

   Cette valeur doit correspondre à 50 % de la taille maximum du segment de mémoire Java.

   Limite de mémoire pour tous les messages

   Cette valeur doit correspondre à 50 % de la taille maximum du segment de mémoire Java.

   Limite de mémoire par file d'attente

   Cette valeur doit être calculée en fonction du nombre d'installations Data Collector dont vous disposez.

   Exemple : Mémoire par file d'attente

   (mémoire du système pour tous les messages)/5/(nombre d'installations Data Collector)

2. Connectez-vous au serveur d'installation de Data Aggregator. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

   Remarque : Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator.*

3. Pour arrêter l'intermédiaire ActiveMQ, exécutez la commande suivante :

   ```
   /etc/init.d/activemq stop
   ```

4. Modifiez la taille de segment de mémoire Java pour ActiveMQ :

   a. Accédez au fichier **activemq** sous broker/apache-activemq-*version*/bin.

   b. Recherchez la ligne qui définit ACTIVEMQ_OPTS_MEMORY.

   c. Définissez -Xms comme taille minimum initiale du segment de mémoire Java.

   d. Définissez -Xmx comme taille maximum du segment de mémoire Java.

   e. Enregistrez le fichier.

5. Modifiez la limite de mémoire d'ActiveMQ pour le contrôle de flux de producteur :

   a. Accédez au fichier activemq.xml sous *répertoire_installation_Data Aggregator*/broker/apache-activemq-*version*/conf file.

   b. Recherchez la ligne suivante et modifiez la valeur de la limite de mémoire pour tous les messages :

   ```
   <memoryUsage limit="valeur"/>
   ```

c. Recherchez la ligne suivante, modifiez la valeur de la limite de mémoire par file d'attente :

```
<policyEntry queue=">" producerFlowControl="true"
memoryLimit="value"/>
```

Remarque : Pour plus d'informations, consultez http://activemq.apache.org/producer-flow-control.html http://activemq.apache.org/producer-flow-control.html.

6. Pour lancer l'intermédiaire ActiveMQ, exécutez la commande suivante :

```
./etc/init.d/activemq start
```

Les nouveaux paramètres sont activés.

Gestion de la conservation de données

Les taux de conservation des données pour le Data Repository sont gérables. Les taux de conservation des données par défaut dans le Data Repository sont définis pour conserver l'espace disque et améliorer la génération de rapports pour la plupart des utilisateurs. Les données interrogées sont générées toutes les 5 minutes par défaut pour une unité ; elles représentent les données les plus détaillées disponibles dans le produit. Un cumul de ces données interrogées brutes est défini à un intervalle d'une heure. Ce cumul des données est en fait un cumul des valeurs interrogées, qui fournissent un niveau de détail moins élevé dans les rapports. Vous pouvez conserver les cumuls quotidiens et hebdomadaires plus longtemps que les données horaires ou les données interrogées, car leur conservation requiert moins d'espace disque.

Toutefois, vous pouvez modifier le taux de conservation des données interrogées par le Data Repository, les données de cumul hebdomadaire, les données de cumul quotidien et les données de cumul horaire. Par exemple, vous pouvez définir la valeur de conservation des données interrogées sur 30 jours afin de l'espace sur le disque. Déterminez la valeur qui convient le mieux à vos besoins et à votre environnement.

Remarque : Pour plus d'informations sur la modification des durées de conservation de données, consultez le *Manuel des services Web REST*.

Par défaut, les données sont conservées dans le Data Repository pour le nombre de jours suivant :

- Données interrogées : 45 jours

  Remarque : Si vous avez mis à niveau vers cette version à partir d'une version précédente de Data Aggregator, la conservation de données interrogée ne changera pas par rapport à la valeur par défaut précédente de dix jours.
- Données de cumul horaire : 90 jours
- Données de cumul quotidien : 365 jours
- Données de cumul hebdomadaire : 730 jours

Nombre minimum de jours pendant lequel le Data Repository peut conserver des données :

- Données interrogées : 2 jours
- Données de cumul horaire : 8 jours
- Données de cumul quotidien : 31 jours
- Données de cumul hebdomadaire : 366 jours

Chapitre 2: Redémarrage des services de composants

Ce chapitre traite des sujets suivants :

Arrêt et redémarrage du Data Aggregator (page 51)
Arrêt et redémarrage de Data Collector (page 53)
Arrêt et redémarrage du Data Repository (page 54)
Arrêt et redémarrage de l'intermédiaire ActiveMQ (page 56)

Arrêt et redémarrage du Data Aggregator

Vous pouvez être amené à arrêter et redémarrer Data Aggregator, par exemple, lorsque le système d'exploitation de l'hôte Data Aggregator requiert une mise à niveau. Arrêtez Data Aggregator, effectuez les actions requises, puis redémarrez Data Aggregator. Data Aggregator reprend alors le traitement.

Pendant un arrêt planifié du Data Aggregator, toutes les données interrogées reçues avant que le Data Aggregator se ferme sont envoyées au Data Repository. Ces données interrogées sont préservées pour la génération de rapports et à d'autres fins.

Tenez compte des informations suivantes concernant le traitement du chargement des données, des cumuls et des événements de seuil lorsque vous envisagez d'arrêter Data Aggregator :

- Toutes les données qui ont été reçues à partir de composants de Data Collector pendant les cycles d'interrogation actuels sont traitées avant que Data Aggregator s'arrête. Les données ne sont pas perdues.
- Si le traitement d'événement de seuil a commencé, au moment de l'arrêt, le traitement des données reçues en provenance des composants Data Collector se termine avant l'arrêt de Data Aggregator.
- Le traitement d'événement de seuil reprend au redémarrage de Data Aggregator.
- Si le traitement de cumul a démarré au moment de l'arrêt, le cumul des données collectées au niveau des hôtes Data Collector se termine avant l'arrêt de Data Aggregator.
- Le traitement de cumul reprend au redémarrage de Data Aggregator.

Data Aggregator peut se fermer d'une manière imprévue, par exemple, si l'ordinateur sur lequel Data Aggregator est installé subit une coupure de courant. Dans ce cas, Data Aggregator s'arrête brusquement. Vous risquez alors de perdre des données interrogées et des informations d'événement de seuil. Le chargement des données mises en file d'attente à partir des hôtes Data Collector reprend lorsque Data Aggregator redémarre. Le traitement de seuil d'événement et du cumul pour les données mises en file d'attente reprend lorsque Data Aggregator redémarre.

Procédez comme suit :

1. Connectez-vous au serveur d'installation de Data Aggregator. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

   Remarque : Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator.*

2. Ouvrez une invite de commande et effectuez l'une des opérations suivantes :

   a. Si vous êtes connecté en tant qu'utilisateur root, entrez la commande suivante :

      ```
      service dadaemon stop
      ```

   b. Si vous êtes connecté en tant qu'utilisateur sudo, entrez la commande suivante :

      ```
      sudo service dadaemon stop
      ```

   L'interrogation se poursuit sur Data Collector s'il est en cours d'exécution et d'interrogation lorsque Data Aggregator est arrêté. Data Collector met en file d'attente les données interrogées pour une remise future à Data Aggregator.

3. Déplacez l'ordinateur ou effectuez toute autre tâche administrative.

4. Connectez-vous au serveur d'installation de Data Aggregator. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

   Remarque : Si vous avez installé Data Aggregator en tant qu'utilisateur sudo, vous avez configuré un alias sudo pour la commande /etc/init.d/dadaemon. Utilisez la commande sudo pour exécuter le script de démarrage de dadaemon. Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator*.

5. Ouvrez une invite de commande et saisissez la commande suivante :

   ```
   service dadaemon start
   ```

   Data Aggregator démarre et se synchronise automatiquement avec CA Performance Center.

Lorsque Data Aggregator démarre, toutes les données interrogées mises en file d'attente sur l'hôte Data Collector sont envoyées à Data Aggregator. Les données les plus récentes sont abandonnées si les données mises en file d'attente dépassent une limite d'espace disque configurée sur le système Data Collector. En conséquence, il y a un espace vide dans les données de rapport interrogées.

Arrêt et redémarrage de Data Collector

Vous pouvez être amené à arrêter et redémarrer Data Collector, par exemple, si l'ordinateur sur lequel Data Collector est installé subit une panne de courant ou se verrouille. Vous pouvez aussi souhaiter déplacer l'ordinateur. Dans ce cas, arrêtez et redémarrez Data Collector. Pour installer un correctif du système d'exploitation, arrêtez et redémarrez Data Collector.

Procédez comme suit :

1. Connectez-vous au serveur sur lequel Data Collector est installé. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

   Remarque : Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator.*

2. Ouvrez une invite de commande et effectuez l'une des opérations suivantes :

   a. Si vous êtes connecté en tant qu'utilisateur root, entrez la commande suivante :

      ```
      service dcmd stop
      ```

   b. Si vous êtes connecté en tant qu'utilisateur sudo, entrez la commande suivante :

      ```
      sudo service dcmd stop
      ```

   Quand Data Collector est arrêté, toutes les interrogations en cours s'arrêtent. Vous ne pouvez pas exécuter de détections.

3. Déplacez l'ordinateur ou effectuez toute autre tâche administrative.
4. Démarrez Data Collector en vous connectant à l'ordinateur sur lequel Data Collector est installé. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

   Remarque : Si vous avez utilisé Data Collector en tant qu'utilisateur sudo, vous avez configuré un alias sudo pour la commande /etc/init.d/dcmd. Utilisez la commande sudo pour exécuter le script de démarrage dcmd. Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator*.
5. Ouvrez une invite de commande et saisissez la commande suivante :

   ```
   service dcmd start
   ```

   Lorsque Data Collector est redémarré, l'interrogation planifiée reprend. Vous pouvez de nouveau exécuter des détections. Data Collector se resynchronise avec CA Performance Center automatiquement.

Informations complémentaires :

Activation des clients hébergés (page 109)

Arrêt et redémarrage du Data Repository

Vous pouvez être amené à arrêter et redémarrer le Data Repository, par exemple, lorsque l'ordinateur sur lequel le Data Repository est installé subit une panne de courant ou se verrouille. Vous pouvez aussi souhaiter déplacer l'ordinateur. Dans de telles circonstances, arrêtez et redémarrez le Data Repository. Pour installer un correctif du système d'exploitation ou procéder à une mise à niveau vers une nouvelle version du Data Repository, arrêtez et redémarrez le Data Repository.

Procédez comme suit :

1. Connectez-vous au serveur d'installation de Data Aggregator. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

   Remarque : Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator.*
2. Ouvrez une invite de commande et saisissez la commande suivante :

   ```
   service dadaemon stop
   ```
3. Connectez-vous au serveur de base de données que vous utilisez pour le Data Repository en tant qu'administrateur de base de données et non *pas* qu'utilisateur root :

4. Saisissez la commande suivante :

   ```
   /opt/vertica/bin/adminTools
   ```

   La boîte de dialogue Administration Tools s'affiche.

5. Sélectionnez (4) Stop Database.
6. Appuyez sur la barre d'espacement à côté du nom de la base de données, sélectionnez OK et appuyez sur Entrée.

   Vous êtes invité à entrer le mot de passe de la base de données.

7. Entrez le mot de passe de base de données et appuyez sur Entrée.

   Le Data Repository s'arrête.

   Remarque : Si Data Repository ne s'arrête pas, sélectionnez (2) Stop Vertica on Host dans (7) Advanced Tools Menu.

8. Sélectionnez Exit et appuyez sur Entrée.
9. Déplacez l'ordinateur ou effectuez toute autre tâche administrative.
10. Connectez-vous au serveur de base de données que vous utilisez pour le Data Repository en tant qu'administrateur de base de données et non *pas* qu'utilisateur root :
11. Saisissez les commandes suivantes :

    ```
    /opt/vertica/bin/adminTools
    ```

    La boîte de dialogue Administration Tools s'affiche.

12. Sélectionnez (3) Démarrer la base de données.
13. Appuyez sur la barre d'espacement à côté du nom de la base de données, sélectionnez **OK** et appuyez sur Entrée.

    Vous êtes invité à entrer le mot de passe de la base de données.

14. Entrez le mot de passe de base de données et appuyez sur Entrée.

    La base de données démarre.

15. Sélectionnez (E) Quitter et appuyez sur Entrée.

16. Démarrez Data Aggregator en vous connectant à l'ordinateur sur lequel Data Aggregator est installé. Connectez-vous en tant qu'utilisateur root ou utilisateur sudo disposant d'un accès à un ensemble limité de commandes.

    Si vous avez installé Data Aggregator en tant qu'utilisateur sudo, vous devez configurer un alias sudo pour la commande service dadaemon. Utilisez la commande sudo pour exécuter le script de démarrage de dadaemon.

    Remarque : Pour plus d'informations sur l'utilisateur sudo, reportez-vous au *Manuel d'installation de Data Aggregator.*

17. Ouvrez une invite de commande et saisissez la commande suivante :

    ```
    service dadaemon start
    ```

    Le Data Repository redémarre.

Arrêt et redémarrage de l'intermédiaire ActiveMQ

Redémarrez l'intermédiaire Apache ActiveMQ si Data Aggregator détecte un problème avec ActiveMQ et ne parvient pas à redémarrer l'intermédiaire. Vous pouvez également arrêter manuellement le service et le redémarrer le cas échéant.

Procédez comme suit :

1. Ouvrez le répertoire suivant à partir de la ligne de commande :
   cd
   répertoire_installation_da/broker/apache-activemq-*version*/bin

   répertoire_installation_da

   Spécifie l'emplacement du répertoire d'installation de Data Aggregator.

   apache-activemq-*version*

   Indique la version d'Apache ActiveMQ.

   Exemple : apache-activemq-5.5.1b

2. Exécutez la commande stop :

```
./activemq stop –jmxurl
service:jmx:rmi:///jndi/rmi://localhost:11099/jmxrmi --jmxuser
admin --jmxpassword activemq da_broker
```

–jmxurl service:jmx:rmi:///jndi/rmi://localhost:11099/jmxrmi

Spécifie l'emplacement de l'intermédiaire activemq. Cet emplacement change uniquement lorsqu'un utilisateur modifie le port ou externalise l'intermédiaire sur un autre système.

Remarque : La modification du numéro de port est prise en charge, mais l'externalisation de l'intermédiaire ne l'est pas.

--jmxuser admin

Spécifie le nom d'utilisateur pour l'arrêt du service.

Valeur par défaut : admin

--jmxpassword activemq

Spécifie le mot de passe pour l'arrêt du service.

Valeur par défaut : activemq

da_broker

Spécifie le nom de l'intermédiaire qui sera arrêté.

Valeur par défaut : da_broker

3. Exécutez la commande start :

```
./activemq start
```

Chapitre 3: Détection de votre réseau

Ce chapitre traite des sujets suivants :

Détection d'unités (page 59)
Flux de travaux de détection (page 60)
Profils SNMP (page 62)
Détection et interrogation (page 63)
Détection et interrogation dans des environnements VMware (page 66)
Profils de détection (page 66)
Exécution de détections à la demande (page 76)
Détections de planification (page 78)
Affichage des résultats de la détection (page 79)
Détection à partir d'autres sources de données (page 81)
Modifications du type d'unité (page 82)
Nouvelle détection (page 84)

Détection d'unités

La *détection* est le processus à travers lequel Data Aggregator détecte et modélise votre infrastructure informatique.

Le processus de détection permet d'effectuer les actions suivantes :

- Confirmer les protocoles auxquels les unités répondent. Data Aggregator détermine toujours si l'unité peut répondre au protocole SNMP. Si vous sélectionnez ICMP, Data Aggregator détermine d'abord si une unité peut répondre à une demande ICMP. Si l'unité *répond* à une demande ICMP, Data Aggregator détermine alors si l'unité peut répondre à une demande SNMP. Si l'unité *ne répond pas* au protocole ICMP, Data Aggregator ne confirmera pas que l'unité répond au protocole SNMP.
- Récupérer un ensemble minimum d'informations concernant toutes les unités détectées qui permet de classer les unités et de les ajouter à la collection appropriée.

Vous pouvez utiliser deux méthodes pour détecter des unités dans Data Aggregator :

- Vous pouvez détecter des unités spécifiques dans votre environnement d'infrastructure à l'aide des profils de détection que vous créez dans Data Aggregator. Suivez les étapes du flux de travaux de détection pour gérer les unités avec cette méthode. (page 60)
- Vous pouvez détecter des unités qui ont été fournies à partir de CA Performance Center (page 81).

Flux de travaux de détection

Le flux de travaux suivant offre une recommandation d'utilisation en tant que référence rapide lors de la détection de votre inventaire.

Effectuez ce processus en tant qu'utilisateur possédant le rôle Administrateur ou en tant qu'administrateur de clients hébergés.

1. Si vous voulez que Data Collector génère des requêtes de tables de base MIB d'unité utilisant le protocole SNMP, créez des profils SNMP dans CA Performance Center avant d'effectuer la détection.

   Remarque : Pour appliquer un profil SNMP à un client hébergé, le profil SNMP doit avoir *été créé* dans l'espace de client hébergé par un utilisateur possédant le rôle d'administrateur de clients hébergés. Pour plus d'informations sur la création des profils SNMP, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

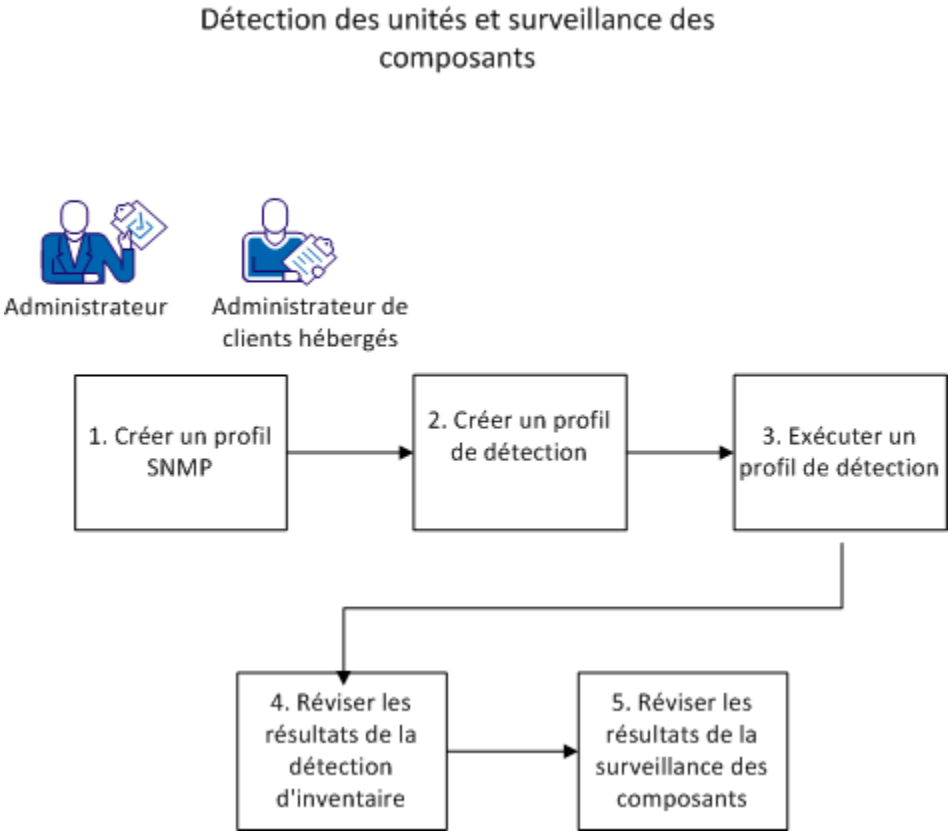
2. Créez un ou plusieurs profils de détection à partir des pages d'administration de Data Ag (page 68)gregator.

3. Exécutez un ou plusieurs profils de détection (page 76). Vous pouvez planifier la détection ou l'exécuter manuellement.

4. Vérifiez les résultats de la détection.

5. Vérifiez les résultats de la surveillance des composants (page 99). Utilisez les résultats pour déterminer le mode de gestion des unités et des composants.

Ce diagramme illustre le processus de détection :



Informations complémentaires :

Détection d'unités (page 59)

Profils SNMP

Les profils SNMP sont des définitions qui contiennent les informations nécessaires pour autoriser Data Collector à interroger les tables de base de données d'informations de gestion d'unité qui utilisent le protocole SNMP. Data Collector peut communiquer avec des unités qui prennent en charge SNMPv1, SNMPv2c et SNMPv3. Les chaînes de communauté et les informations d'identification sont chiffrées lorsqu'elles sont stockées dans CA Performance Center et lorsqu'elles sont envoyées à Data Aggregator et à Data Collector.

Important : En cas d'utilisation de noms de communauté SNMPv3, CA Infrastructure Management requiert l'utilisation de mots de passe d'authentification ou de confidentialité de plus de huit caractères. Si les mots de passe contiennent moins de huit caractères, les profils SNMPV3 ne permettront peut-être pas de communiquer avec les unités.

Data Collector utilise les profils SNMPv1/SNMPv2c et SNMPv3 pendant la détection d'inventaire pour définir les informations d'identification à utiliser lors de l'accès à une unité. CA Performance Center se charge de gérer cette liste de profils. Un classement est associé à chaque profil pour l'accès à l'unité. Pendant la détection, l'accès à l'unité est testé pour chaque profil. Le profil dont le classement est le plus élevé pour l'accès à une unité est utilisé.

Vous pouvez créer des profils SNMP dans CA Performance Center et vous pouvez modifier le classement des profils SNMP. Une nouvelle liste de profils SNMP classés prend effet dans les situations suivantes :

- Une nouvelle unité est détectée.
- Une unité existante cesse d'être accessible via le protocole SNMP pendant au moins deux cycles d'interrogation.
- Le profil SNMP qu'une unité utilise est supprimé de CA Performance Center.

Dans le cas contraire, les unités qui sont déjà interrogées continuent d'utiliser le profil SNMP existant, indépendamment de toute modification que vous avez apportée à la liste de profils SNMP.

Remarque : Si le profil SNMPv1/SNMPv2c est le plus élevé qui puisse accéder à une unité et que l'unité est accessible avec SNMPv1 et SNMPv2c, Data Collector communique avec cette unité en utilisant SNMPv2c.

Nous avons testé Data Collector pour déterminer la charge d'UC ajoutée lorsque divers protocoles SNMPv3 sont utilisés. Nous avons constaté que SHA/AES entraînait un impact modéré (< 30 %) sur l'utilisation d'UC par rapport à SNMPv1. Nous avons également remarqué que le MD5/DES, le SHA/DES, et le SHA/3DES ont un impact majeur (>30 %) sur l'utilisation de l'UC.

Remarque : Les serveurs sur lesquels cette analyse a été effectuée possèdent certaines aptitudes d'AES intégrées aux UC.

Si vous ajoutez des noyaux d'UC supplémentaires à votre environnement, Data Collector peut équilibrer la charge d'UC.

Vous créez des profils SNMP dans l'interface utilisateur de CA Performance Center ou à l'aide des services Web REST de CA Performance Center. Après la création des profils SNMP, ceux-ci sont immédiatement synchronisés avec Data Aggregator et peuvent être utilisés par la détection d'inventaire.

Remarque : Pour plus d'informations sur la création de profils SNMP, reportez-vous au *Manuel de l'administrateur de CA Performance Center* et au *Manuel des services Web REST de CA Performance Center*.

Après la détection, vous pouvez accéder à la vue Historique de détection pour consulter la liste des profils SNMP utilisés et le profil SNMP le mieux classé auquel l'unité a répondu.

Informations complémentaires :

Affichage des résultats de la détection (page 79)

Détection et interrogation

La *détection* est le processus à travers lequel Data Aggregator détecte et modélise votre infrastructure informatique.

Le processus de détection permet d'effectuer les actions suivantes :

- Confirmer les unités auxquelles les protocoles répondent, en fonction des protocoles que vous sélectionnez lorsque vous créez un profil de détection. Par exemple, si vous sélectionnez tous les protocoles (SNMP et ICMP), les opérations suivantes sont effectuées : Data Aggregator détermine si l'unité peut répondre à une demande ICMP, puis si l'unité peut répondre à une demande SNMP. Si l'unité *ne répond pas* au protocole ICMP, Data Aggregator ne confirmera pas que l'unité répond au protocole SNMP.
- Récupérer un ensemble minimum d'informations concernant toutes les unités détectées qui permet de classer les unités et de les ajouter à la collection appropriée.

La détection d'inventaire correspond au processus d'identification des unités de votre réseau par Data Aggregator. Les unités sont identifiées à l'aide du domaine IP, des adresses IP, des plages d'adresses IP et des noms d'hôte que vous spécifiez dans les profils de détection. La détection d'inventaire permet d'identifier si les unités sont gérables ou pas (si elles acceptent la commande ping ou si elles utilisent le protocole SNMP) et de les classer (routeur, commutateur, etc.). La détection d'inventaire détermine également le fournisseur (Cisco, Juniper, etc.) et le type (7700, 8200, etc.).

Les unités détectées pendant ce processus sont automatiquement ajoutées à des collections prêtes à l'emploi, sur la base des règles de contrôle de l'appartenance de chaque collection d'unités. Vous pouvez également créer des collections d'unités personnalisées dans CA Performance Center : celles-ci se chargent de créer les collections personnalisées correspondantes dans Data Aggregator lors de la synchronisation. Au cours de la première synchronisation avec CA Performance Center et suite à leur *détection*, les unités sont ajoutées à des collections d'unités personnalisées en fonction des règles définies pour ces collections.

Remarque : Pour plus d'informations sur la création de collections d'unités personnalisées et leur synchronisation avec Data Aggregator, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

La surveillance de composants est un processus distinct. Le processus de surveillance implique la collecte et l'analyse de diverses données opérationnelles concernant des composants d'unité spécifiques, notamment l'UC, la mémoire et les interfaces. Toutes les informations qui décrivent le processus de surveillance se trouvent dans les profils de surveillance que vous assignez aux collections d'unités.

La relation entre les profils de surveillance et les collections d'unités régit la surveillance des composants. La surveillance de composants peut être déclenchée de plusieurs manières :

- Un profil de surveillance est assigné à une collection d'unités dont une unité donnée est membre.
- Une unité est ajoutée à une collection à laquelle un profil de surveillance est déjà assigné.
- Un profil de surveillance, qui est assigné à une collection d'unités, est modifié pour inclure une nouvelle famille de mesures à surveiller. Les composants qui sont associés à la famille de mesures sont ensuite surveillés automatiquement pour chaque unité dans la collection à laquelle le profil de surveillance est rattaché, si le composant n'a pas été surveillé préalablement pour l'unité.
- Une nouvelle certification de fournisseur est ajoutée pour une famille de mesures existante interrogée dans un profil de surveillance.

- Un profil de surveillance spécifie un taux de détection des modifications et l'option Mise à jour automatique des familles de mesures est activée.
- Dans l'onglet Familles de mesures interrogées de la vue Unités surveillées, cliquez sur le bouton Mettre à jour la famille de mesures.

Une *famille de mesures* définit l'ensemble de valeurs permettant de collecter et de générer des rapports pour une technologie donnée. Ces valeurs sont normalisées afin d'uniformiser la génération de rapports indépendamment de la source de données. Lorsqu'elles sont incluses dans un profil de surveillance, les familles de mesures déterminent quelles valeurs collecter pour les unités associées à ce profil de surveillance.

L'interrogation commence automatiquement à la fin de la détection d'inventaire et de la surveillance des composants. Les mesures opérationnelles et les données de configuration sont interrogées sur l'unité détectée et leurs composants surveillés. Les mesures opérationnelles et les données de configuration qui sont interrogées dépendent des familles de mesures que vous spécifiez dans le profil de surveillance. Les mesures opérationnelles sont collectées et conservées à intervalle régulier à des fins de rapport. Les exemples de mesures opérationnelles comprennent le taux d'erreurs, la référence quotidienne, la référence horaire et les performances de port. Les données de configuration représentent ou identifient un composant ou la configuration du composant.

Exemples de données de configuration :

ifNumber

Variable de base de données d'informations de gestion qui indique à Data Aggregator de combien de ports dispose une unité.

ifStackLastChange

Une variable MIB qui indique si une modification se produit sur une table de pile d'interface.

Un délai de 5 minutes est requis avant la synchronisation des unités détectées et des composants surveillés avec CA Performance Center. Les unités et les composants détectés et surveillés pendant une synchronisation sont synchronisés à l'issue de la synchronisation en cours.

Informations complémentaires :

Affichage des unités surveillées (page 99)
Gestion de la détection des modifications (page 110)

Détection et interrogation dans des environnements VMware

Vous pouvez détecter et surveiller vos ordinateurs virtuels VMware et vos hôtes ESX en même temps que vos périphériques réseau. Bien que les composants et les unités VMware fonctionnent comme des composants physiques, le processus de détection et de surveillance de ces unités et ces composants est différent pour permettre la collection des données à partir du serveur vCenter. Outre la détection des ordinateurs virtuels et des hôtes ESX directement avec SNMP, il est également possible de collecter des données vCenter à l'aide du module VCAIM (vCenter Server Application Insight Module).

Vous pouvez détecter des hôtes ESX et des ordinateurs virtuels dans votre environnement VMware.

Pendant la détection d'inventaire, Data Aggregator identifie les ordinateurs virtuels et les hôtes ESX des façons suivantes :

- Par le protocole ICMP
- Par le protocole SNMP, si les serveurs incluent un agent SNMP déployé.
- Par la détection d'un serveur exécutant systemEdge avec le module VCAIM

Bien que vous puissiez identifier chaque hôte et ordinateur virtuel ESX plusieurs fois à l'aide du protocole ICMP ou SNMP et du serveur vCenter, seul une unité est créée. Cette unité représente l'ordinateur virtuel ou l'hôte ESX.

Une fois les unités d'ordinateur virtuel et ESX créées, Data Aggregator lance l'interrogation des mesures spécifiques d'un serveur vCenter et peut détecter et démarrer l'interrogation de composants supplémentaires identifiés par l'agent SNMP.

Selon la source des données de mesure, certaines interrogations pour les ordinateurs virtuels et ESX ont lieu directement sur l'unité, alors que le module VCAIM est interrogé pour collecter d'autres données.

Par défaut, toutes les 15 minutes (soit après avoir détecté votre environnement VMware), le Data Aggregator surveille les ordinateurs virtuels qui ont été ajoutés ou supprimés ou qui ont été déplacés virtuellement d'un hôte ESX à un autre. Par défaut, toutes les 24 heures, le Data Aggregator surveille également si des hôtes ESX ont été ajoutés ou supprimés.

Profils de détection

Les profils de détection spécifient la procédure de détection d'inventaire. En tant qu'administrateur, vous pouvez utiliser l'interface utilisateur de CA Performance Center ou les services Web REST de Data Aggregator pour gérer les profils de détection.

Dans un profil de détection, vous spécifiez les adresses IP, les plages d'adresses IP et les noms d'hôte pour lesquels vous souhaitez détecter des unités. Vous spécifiez également un domaine IP. Vous pouvez uniquement spécifier un domaine IP pour chaque profil de détection que vous créez. Les nouvelles unités détectées seront créées dans ce domaine IP.

Lorsque plusieurs hôtes Data Collector sont déployés dans un domaine IP, chaque hôte Data Collector envoie une demande de détection à cette unité.

Lorsque plusieurs hôtes Data Collector peuvent contacter la même unité, un serveur spécifique Data Collector est sélectionné pour surveiller l'unité. Un algorithme, défini selon l'équilibrage de la charge, détermine cette sélection.

Les domaines IP sont également nécessaires pour la surveillance des environnements de client hébergé dont les adresses IP se chevauchent. Un client hébergé peut avoir un ou plusieurs domaines IP. Si un client hébergé possède des adresses IP qui se chevauchent, il doit y avoir plusieurs domaines IP dans le réseau. Les adresses IP qui se chevauchent sont gérées via des domaines IP.

Les domaines IP sont créés dans CA Performance Center. Data Aggregator prend connaissance des nouveaux domaines IP lorsque la synchronisation manuelle ou automatique se produit.

Le processus de détection tente de distribuer les unités sur les instances de Data Collector disponibles, sans tenir compte des unités qu'une instance de Data Collector surveille actuellement.

Remarque : Pour plus d'informations sur la création et la synchronisation des domaines IP, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

Les profils de détection sont uniquement accessibles par les utilisateurs qui se trouvent dans l'espace de client hébergé dans lequel le profil de détection a été créé. Un utilisateur assigné à l'espace Client hébergé par défaut peut exécuter une détection à l'aide d'un profil de détection présent au niveau de l'espace Client hébergé par défaut et afficher les résultats de cette détection.

Par conséquent, il est important d'être connecté en tant que client hébergé ou d'administrer le client hébergé correct *avant* de créer un profil de détection.

Remarque : Pour plus d'informations sur la création et l'administration des clients hébergés, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

Informations complémentaires :

Création de profils de détection (page 68)
Suppression des profils de détection (page 76)
Modification des profils de détection (page 73)
Affichage d'une liste de profils de détection (page 68)
Suppressions de domaine IP (page 106)

Affichage d'une liste de profils de détection

Les profils de détection pour SNMP et ICMP permettent de configurer la procédure de détection dans votre environnement.

Vous pouvez afficher une liste de profils de détection et les détails de chacun. Vous pouvez afficher le statut de détection et l'heure de la dernière exécution de la détection. Ces détails aident à comprendre comment votre réseau est détecté.

Remarque : Connectez-vous comme administrateur de clients hébergés pour effectuer cette tâche.

Procédez comme suit :

1. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.
2. Cliquez sur Profils de détection dans le menu Inventaire surveillé.

   La page Liste de profils de détection s'ouvre. Elle contient la liste des profils de détection disponibles.

Informations complémentaires :

Plages d'adresses IP de profil de détection (page 71)
Création de profils de détection (page 68)
Suppression des profils de détection (page 76)
Modification des profils de détection (page 73)
Exécution de détections à la demande (page 76)
Détections de planification (page 78)
Profils de détection (page 66)
Affichage des résultats de la détection (page 79)

Création de profils de détection

Vous pouvez créer des profils de détection pour spécifier la procédure de détection d'inventaire dans votre environnement.

Connectez-vous comme administrateur de clients hébergés pour effectuer cette tâche. Les profils de détection sont uniquement accessibles par les utilisateurs qui se trouvent dans l'espace de client hébergé dans lequel le profil de détection a été créé.

Remarque : Pour en savoir plus sur les clients hébergés, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

Procédez comme suit :

1. Accédez à la liste de profils de détection disponibles (page 68).
2. Cliquez sur Créer.
3. Procédez comme suit :
   a. Dans le champ Nom, indiquez un nom du profil de détection.

      Remarque : Les apostrophes simples, les apostrophes doubles, les barres obliques inverses, les barres obliques et les esperluettes ne sont pas autorisées.

   b. Sélectionnez un domaine IP dans la liste de domaines pré-configurés.
4. Sélectionnez l'onglet Adresses IP/Hôtes et effectuez l'une des opérations suivantes :
   - (Facultatif) Accédez à un fichier CSV d'adresses IP et importez-le. Le fichier CSV peut contenir une liste séparée par des virgules d'adresses IPv4, adresses IPv6, de plages d'adresses IPv4 et de noms d'hôte. Sélectionnez le fichier, puis cliquez sur Ouvrir.

     Remarque : Pour que les caractères chinois soient appliqués au nom d'alias, enregistrez le fichier CSV au format UTF-8.
   - Saisissez des plages d'adresse IP pour lesquelles vous souhaitez détecter des unités dans le champ Plage d'adresses IP. Les valeurs séparées par des virgules sont acceptées.

     Remarque : Si une plage d'adresses IP inclut plusieurs adresses IP pour une unité qui possède un nom d'hôte et si l'adresse IP qui mappe vers le nom d'hôte est également incluse dans la plage d'adresses IP, la détection d'inventaire utilise systématiquement l'adresse IP de nom d'hôte pour l'adresse IP principale de l'unité.
   - Saisissez des adresses IP distinctes pour lesquelles vous souhaitez détecter des unités dans le champ Liste d'adresses IP. Les valeurs séparées par des virgules sont acceptées.
   - Saisissez les noms d'hôte pour lesquels vous souhaitez détecter des unités dans le champ Liste des hôtes. Les valeurs séparées par des virgules sont acceptées.
   - Copiez une liste d'adresses IP individuelles, de plages d'adresses IP et de noms d'hôte dans le presse-papiers, puis collez-la dans la vue Liste en appuyant sur les touches Ctrl + C.

- Pour supprimer un élément de la liste d'adresses IP, sélectionnez l'adresse IP, la plage d'adresses IP, ou le nom d'hôte et cliquez sur Supprimer.
- Pour rechercher un élément dans la liste d'adresses IP, entrez l'adresse IP, la plage d'adresses IP, ou le nom d'hôte dans le champ Rechercher. Pour revenir à la liste complète des éléments dans la liste d'adresses IP, cliquez sur le signe X. Vous pouvez également appuyer sur la touche Echap de votre clavier.

Remarque : Pour modifier une adresse IP, une plage d'adresses IP ou un nom d'hôte dans la liste d'adresses IP, double-cliquez dessus. Pour enregistrer les modifications, appuyez sur la touche Entrée. Pour quitter le mode d'édition sans enregistrer les modifications, appuyez sur la touche Echap.

N'incluez pas d'adresses IP ou de noms d'hôte en double. Si des doublons sont détectés, un message s'affiche, indiquant que les doublons ont été identifiés et ignorés.

Remarque : Les apostrophes simples, les apostrophes doubles, les barres obliques inverses, les barres obliques et les esperluettes ne sont pas autorisées.

5. (Facultatif) Sélectionnez l'onglet Planification. Pour créer une planification d'exécution du profil de détection, procédez comme suit :
   - Pour créer une planification quotidienne, déroulez la liste Intervalle de planification et sélectionnez Quotidienne. Sélectionnez l'heure à laquelle vous souhaitez que la détection commence chaque jour.
   - Pour créer une planification hebdomadaire, déroulez la liste Intervalle de planification et sélectionnez Hebdomadaire. Sélectionnez les jours d'exécution de la détection. Sélectionnez l'heure à laquelle vous souhaitez que la détection commence.
6. Cliquez sur l'onglet SNMP. Si vous voulez utiliser tous les profils SNMP, aucune action n'est requise de votre part. En effet, tous les profils SNMP sont sélectionnés par défaut. Pour utiliser des profils SNMP spécifiques, sélectionnez l'option Utiliser une liste spécifique des profils SNMP assignés. Dans la liste de profils disponibles, sélectionnez un ou plusieurs profils SNMP et déplacez-les vers la liste des profils affectés. L'utilisation d'un sous-ensemble de profils SNMP peut aider à réduire le trafic réseau.
7. Sélectionnez l'onglet Avancé et effectuez les opérations suivantes :
   a. (Facultatif) Changez la priorité de nommage de l'unité détectée. Pendant la détection, les éléments d'unité créés par le profil de détection sont nommés selon la convention d'attribution de nom la plus élevée disponible. Si une convention d'attribution de nom n'est pas définie dans la MIB pour l'unité, elle n'est pas disponible et la convention de niveau de priorité suivant est utilisée.
   b. (Facultatif) Sélectionnez l'option Enregistrer en tant que valeur par défaut, si vous voulez enregistrer l'ordre d'attribution des noms pour les *nouveaux profils de détection*. Ainsi, lorsque vous créez un profil de détection, les noms s'affichent automatiquement dans l'ordre dans lequel ils ont été enregistrés.

L'ordre d'attribution des noms par défaut est Nom du système, Nom d'hôte, Adresse IP.

c. Si vous souhaitez que Data Aggregator détermine si une unité peut répondre à une demande ICMP lors du processus de détection, sélectionnez l'option Utiliser ICMP. Pour créer des unités acceptant la commande ping pendant la détection, sélectionnez Créer des éléments acceptant la commande ping. Pour empêcher la création d'unités acceptant la commande ping, désélectionnez l'option Utiliser ICMP. Data Aggregator ne détermine pas si une unité peut répondre à une demande ICMP lorsque ces options sont désélectionnées.

   Pour enregistrer les options de détection ICMP que vous avez choisies, sélectionnez Enregistrer en tant que valeur par défaut. Ainsi, lorsque vous créez un profil de détection, les options de détection ICMP sont automatiquement sélectionnées.

8. Cliquez sur Enregistrer.

   Le profil de détection est créé et affiché dans la liste Profils de détection.

Informations complémentaires :

Plages d'adresses IP de profil de détection (page 71)
Flux de travaux de détection (page 60)
Profils de détection (page 66)

Plages d'adresses IP de profil de détection

Lorsque vous créez un profil de détection, vous pouvez entrer les plages d'adresses IP que vous voulez détecter pour IPv4. La détection de plage d'adresses IPv6 n'est pas prise en charge.

Lorsque vous spécifiez des plages d'adresses IP dans le profil de détection, les règles suivantes s'appliquent :

- Une plage IPv4 peut contenir des caractères génériques (*****). Un caractère générique représente une plage complète pour un octet d'adresse IP : 0-255.
- Une plage IPv4 peut contenir des traits d'union (**-**). Un trait d'union peut exister entre l'adresse IP la plus faible et l'adresse IP la plus élevée. Un trait d'union peut également figurer dans les octets IP dans l'adresse IP la plus faible.
- Si un caractère générique ou un trait d'union est utilisé dans un octets de l'adresse IP la plus faible, vous ne pouvez pas représenter l'adresse IP la plus élevée.

Exemples : plages d'adresses IP valides

- Les deux exemples suivants tentent de détecter des unités sur toutes les adresses IP de 10.25.1.0 à 10.25.1.190 :

  `10.25.1.0-10.25.1.190`

  OU
  `10.25.1.0-190`

- Les deux exemples suivants tentent de détecter des unités sur toutes les adresses IP de 10.25.0.0 à 10.25.255.255 :

  `10.25.*.*`

  OU

  `10.25.0.0 - 10.25.255.255`

- Les deux exemples suivants tentent de détecter des unités sur toutes les adresses IP de 10.25.0.3 à 10.25.0.40 et de 10.25.1.3 à 10.25.1.40 :

  `10.25.0-1.3-40`

  OU

  `10.25.0.3 - 10.25.0.40, 10.25.1.3 - 10.25.1.40`

- Les deux exemples suivants tentent de détecter des unités sur toutes les adresses IP de 10.25.0.0 à 10.25.0.5, de 10.25.1.0 à 10.25.1.5, etc., jusqu'à 10.25.255.0 à 10.25.255.5 :

  `10,25.*.0-5`

  OU

  `10.25.0.0 - 10.25.0.5, 10.25.1.0 - 10.25.1.5 ... 10.25.255.0 - 10.25.255.5`

Exemples : plages d'adresses IP non valides

- L'exemple suivant n'est pas valide, car l'adresse IP la plus élevée est incomplète :

  `10.25.1.0 - 10.23`

- L'exemple suivant n'est pas valide, car l'adresse IP la plus élevée ne peut pas être présente lorsqu'un trait d'union (-) est utilisé dans un octet de l'adresse IP la plus faible :

  `10.25.1.0-190 - 10.25.1.255`

- L'exemple suivant n'est pas valide, car l'adresse IP la plus élevée ne peut pas être présente lorsqu'un caractère générique (*) est utilisé dans un octet de l'adresse IP la plus faible :

  `10.25.*.0 - 10.25.255.255`

- L'exemple suivant n'est pas valide, car l'octet de caractère générique (1*) peut signifier 10.25.10-19.0 ou 10.25.10-199.0 :

  `10.25.1*.0`

Informations complémentaires :

Création de profils de détection (page 68)
Affichage d'une liste de profils de détection (page 68)

Modification des profils de détection

Vous pouvez modifier un profil de détection existant.

Remarque : Connectez-vous comme administrateur de clients hébergés pour effectuer cette tâche.

Procédez comme suit :

1. Accédez à la liste de profils de détection disponibles (page 68).
2. Sélectionnez le profil de détection que vous souhaitez modifier, puis cliquez sur Modifier. Apportez les modifications de votre choix dans les champs des onglets.
3. Procédez comme suit :
   a. Dans le champ Nom, indiquez un nom du profil de détection.

      Remarque : Les apostrophes simples, les apostrophes doubles, les barres obliques inverses, les barres obliques et les esperluettes ne sont pas autorisées.

   b. Sélectionnez un domaine IP dans la liste de domaines pré-configurés.

      Remarque : Si vous avez déjà exécuté une détection sur ce profil de détection, vous ne pouvez pas modifier le domaine IP.
4. Sélectionnez l'onglet Adresses IP/Hôtes et effectuez l'une des opérations suivantes :
   - (Facultatif) Accédez à un fichier CSV d'adresses IP et importez-le. Le fichier CSV peut contenir une liste séparée par des virgules d'adresses IPv4, adresses IPv6, de plages d'adresses IPv4 et de noms d'hôte. Sélectionnez le fichier, puis cliquez sur Ouvrir.

     Remarque : Pour que les caractères chinois soient appliqués au nom d'alias, enregistrez le fichier CSV au format UTF-8.

   - Saisissez des plages d'adresse IP pour lesquelles vous souhaitez détecter des unités dans le champ Plage d'adresses IP. Les valeurs séparées par des virgules sont acceptées.

     Remarque : Si une plage d'adresses IP inclut plusieurs adresses IP pour une unité qui possède un nom d'hôte et si l'adresse IP qui mappe vers le nom d'hôte est également incluse dans la plage d'adresses IP, la détection d'inventaire utilise systématiquement l'adresse IP de nom d'hôte pour l'adresse IP principale de l'unité.

- Saisissez des adresses IP distinctes pour lesquelles vous souhaitez détecter des unités dans le champ Liste d'adresses IP. Les valeurs séparées par des virgules sont acceptées.
- Saisissez les noms d'hôte pour lesquels vous souhaitez détecter des unités dans le champ Liste des hôtes. Les valeurs séparées par des virgules sont acceptées.
- Copiez une liste d'adresses IP individuelles, de plages d'adresses IP et de noms d'hôte dans le presse-papiers, puis collez-la dans la vue Liste en appuyant sur les touches Ctrl + C.
- Pour supprimer un élément de la liste d'adresses IP, sélectionnez l'adresse IP, la plage d'adresses IP, ou le nom d'hôte et cliquez sur Supprimer.
- Pour rechercher un élément dans la liste d'adresses IP, entrez l'adresse IP, la plage d'adresses IP, ou le nom d'hôte dans le champ Rechercher. Pour revenir à la liste complète des éléments dans la liste d'adresses IP, cliquez sur le signe X. Vous pouvez également appuyer sur la touche Echap de votre clavier.

Remarque : Pour modifier une adresse IP, une plage d'adresses IP ou un nom d'hôte dans la liste d'adresses IP, double-cliquez dessus. Pour enregistrer les modifications, appuyez sur la touche Entrée. Pour quitter le mode d'édition sans enregistrer les modifications, appuyez sur la touche Echap.

N'incluez pas d'adresses IP ou de noms d'hôte en double. Si des doublons sont détectés, un message s'affiche, indiquant que les doublons ont été identifiés et ignorés.

Remarque : Les apostrophes simples, les apostrophes doubles, les barres obliques inverses, les barres obliques et les esperluettes ne sont pas autorisées.

5. (Facultatif) Sélectionnez l'onglet Planification. Pour créer une planification d'exécution du profil de détection, procédez comme suit :
   - Pour créer une planification quotidienne, déroulez la liste Intervalle de planification et sélectionnez Quotidienne. Sélectionnez l'heure à laquelle vous souhaitez que la détection commence chaque jour.
   - Pour créer une planification hebdomadaire, déroulez la liste Intervalle de planification et sélectionnez Hebdomadaire. Sélectionnez les jours d'exécution de la détection. Sélectionnez l'heure à laquelle vous souhaitez que la détection commence.
6. Cliquez sur l'onglet SNMP. Si vous voulez utiliser tous les profils SNMP, aucune action n'est requise de votre part. En effet, tous les profils SNMP sont sélectionnés par défaut. Pour utiliser des profils SNMP spécifiques, sélectionnez l'option Utiliser une liste spécifique des profils SNMP assignés. Dans la liste de profils disponibles, sélectionnez un ou plusieurs profils SNMP et déplacez-les vers la liste des profils affectés. L'utilisation d'un sous-ensemble de profils SNMP peut aider à réduire le trafic réseau.

7. Sélectionnez l'onglet Avancé et effectuez les opérations suivantes :

   a. (Facultatif) Changez la priorité de nommage de l'unité détectée. Pendant la détection, les éléments d'unité créés par le profil de détection sont nommés selon la convention d'attribution de nom la plus élevée disponible. Si une convention d'attribution de nom n'est pas définie dans la MIB pour l'unité, elle n'est pas disponible et la convention de niveau de priorité suivant est utilisée.

   b. (Facultatif) Sélectionnez l'option Enregistrer en tant que valeur par défaut, si vous voulez enregistrer l'ordre d'attribution des noms pour les *nouveaux profils de détection*. Ainsi, lorsque vous créez un profil de détection, les noms s'affichent automatiquement dans l'ordre dans lequel ils ont été enregistrés.

      L'ordre d'attribution des noms par défaut est Nom du système, Nom d'hôte, Adresse IP.

   c. Si vous souhaitez que Data Aggregator détermine si une unité peut répondre à une demande ICMP lors du processus de détection, sélectionnez l'option Utiliser ICMP. Pour créer des unités acceptant la commande ping pendant la détection, sélectionnez Créer des éléments acceptant la commande ping. Pour empêcher la création d'unités acceptant la commande ping, désélectionnez l'option Utiliser ICMP. Data Aggregator ne détermine pas si une unité peut répondre à une demande ICMP lorsque ces options sont désélectionnées.

      Pour enregistrer les options de détection ICMP que vous avez choisies, sélectionnez Enregistrer en tant que valeur par défaut. Ainsi, lorsque vous créez un profil de détection, les options de détection ICMP sont automatiquement sélectionnées.

8. Cliquez sur Enregistrer.

   Le profil de détection est mis à jour avec vos modifications. Vos modifications seront appliquées lors de la prochaine exécution de ce profil de détection.

Informations complémentaires :

Dépannage : la détection ne démarre pas (page 169)
Profils de détection (page 66)

Suppression des profils de détection

Vous pouvez supprimer un profil de détection dont vous n'avez plus besoin. Par exemple, vous pouvez supprimer des profils de détection qui ne sont plus utilisés, qui sont dupliqués, etc. Vous ne pouvez pas redétecter les unités qui sont spécifiées dans un profil de détection supprimé.

Remarque : Connectez-vous comme administrateur de clients hébergés pour effectuer cette tâche.

Procédez comme suit :

1. Accédez à la liste de profils de détection.
2. Sélectionnez le profil de détection que vous souhaitez supprimer et cliquez sur Supprimer.

   Une boîte de dialogue de confirmation s'ouvre.
3. Cliquez sur Oui.

   Le profil de détection est supprimé.

Exécution de détections à la demande

La détection d'inventaire est le processus permettant de détecter les unités sur votre réseau. Il utilise les informations que vous ajoutez aux profils de détection. Vous pouvez exécuter une détection à la demande.

Les tentatives de détection des unités s'effectuent via des protocoles SNMP et ICMP. Si une unité ne répond pas à SNMP avec les profils SNMPv1/SNMPv2c ou SNMPv3 que vous avez créés, mais *répond* à ICMP, une unité acceptant la commande ping est créée. (Les profils SNMP sont créés à l'aide de l'interface utilisateur de CA Performance Center ou à l'aide des services Web REST de CA Performance Center.)

Vous pouvez effectuer cette tâche en tant qu'administrateur de clients hébergés ou en tant qu'administrateur. Pour exécuter une détection en tant qu'administrateur, configurez Data Collector pour le domaine Client hébergé par défaut avant d'exécuter la détection.

Remarque : Pour plus d'informations sur la création des profils SNMP et de leur synchronisation avec Data Aggregator, reportez-vous au *Manuel de l'administrateur de CA Performance Center* et *au Manuel des services Web REST de CA Performance Center*.

Procédez comme suit :

1. Accédez à la liste de profils de détection dans CA Performance Center (page 68).

2. Sélectionnez un ou plusieurs profils de détection sur lesquels vous souhaitez exécuter une détection et cliquez sur Exécuter.

   Remarque : Vous pouvez uniquement exécuter une détection sur un profil de détection qui est à l'état PRET.

   Une boîte de dialogue de confirmation s'ouvre.

3. Cliquez sur Yes (Oui).

   La détection démarre, la colonne d'état pour les profils de détection sélectionnés indique EN COURS D'EXECUTION et la colonne d'heure de dernière exécution est mise à jour lorsque la détection démarre.

   Remarque : Pour déclencher la colonne Pourcentage d'avancement pendant que la détection s'exécute, cliquez sur Actualiser.

   Une boîte de dialogue de confirmation s'ouvre.

4. Cliquez sur OK.

   Les unités détectées sont ajoutées à des collections d'unités, ce qui initialise la détection et l'interrogation des composants. La page Profil de détection s'affiche de nouveau.

   Si la détection se bloque pendant plus de 10 minutes, elle est interrompue. Une détection est considérée comme bloquée lorsqu'aucune nouvelle unité n'est détectée durant une période de 10 minutes *et* que l'état des profils de détection sélectionnés n'a pas changé depuis 10 minutes. Un événement d'audit est généré sur l'unité Data Aggregator.

   La colonne d'état des profils de détection sélectionnés indique Echec si aucune unité n'a été détectée, ou Echec partiel si au moins une unité a été détectée.

   La synchronisation avec CA Performance Center des composants surveillés et des unités détectées peut prendre jusqu'à 5 minutes. Lorsque la synchronisation est terminée, les unités détectées et les composants surveillés s'affichent dans l'onglet Inventaire de CA Performance Center.

5. (Facultatif) Pour synchroniser des unités détectées et des composants surveillés immédiatement avec CA Performance Center, procédez comme suit :

   a. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.

   b. Cliquez sur Data Aggregator dans le menu Statut du système.

   c. Sélectionnez Data Aggregator et cliquez sur le bouton Resynchroniser.

Informations complémentaires :

Flux de travaux de détection (page 60)
Méthode de définition et d'activation d'un filtre d'interface (page 129)

Détections de planification

La détection d'inventaire est le processus permettant de détecter les unités sur votre réseau. Il utilise les informations que vous ajoutez aux profils de détection. Vous pouvez planifier une détection pour une exécution quotidienne ou hebdomadaire.

Remarque : Vous pouvez exécuter une détection planifiée à tout moment en sélectionnant un profil de détection et en cliquant sur Exécuter. Toutefois, vous ne pouvez pas initialiser une détection à la demande pour un profil de détection lorsqu'une détection planifiée pour le profil de détection est en cours.

Les tentatives de détection des unités s'effectuent via des protocoles SNMP et ICMP. Si une unité ne répond pas à SNMP avec les profils SNMPv1/SNMPv2c ou SNMPv3 que vous avez créés, mais *répond* à ICMP, une unité acceptant la commande ping est créée. (Les profils SNMP sont créés à l'aide de l'interface utilisateur de CA Performance Center ou à l'aide des services Web REST de CA Performance Center.)

Pour exécuter une détection en tant qu'administrateur, configurez Data Collector pour le domaine Client hébergé par défaut avant de planifier la détection.

Remarque : Pour plus d'informations sur la création des profils SNMP et de leur synchronisation avec Data Aggregator, reportez-vous au *Manuel de l'administrateur de CA Performance Center* et *au Manuel des services Web REST de CA Performance Center*.

Procédez comme suit :

1. Accédez à la liste de profils de détection dans CA Performance Center (page 68).
2. Effectuez l'une des opérations suivantes :
   - Sélectionnez un profil de détection existant pour lequel vous voulez planifier une détection et cliquez sur Modifier.

     La page Modifier le profil de détection s'ouvre.
   - Cliquez sur Créer pour créer un profil de détection pour lequel vous voulez planifier une détection.

     La boîte de dialogue Profils de détection s'affiche.
3. Pour créer une planification d'exécution du profil de détection, effectuez l'une des opérations suivantes :
   - Pour créer une planification quotidienne, sélectionnez Exécution quotidienne dans la liste déroulante Intervalle de planification, puis sélectionnez l'heure à laquelle vous souhaitez que la détection commence chaque jour.
   - Pour créer une planification hebdomadaire, sélectionnez Exécution hebdomadaire dans la liste déroulante Intervalle de planification, puis sélectionnez la date à laquelle vous souhaitez que la détection commence.

   Remarque : Sélectionnez Aucune dans la liste déroulante Planification pour supprimer une planification.

4. Cliquez sur Enregistrer.

   Lorsque la détection est planifiée, la colonne Etat du profil de détection indique Planifié et l'heure d'exécution planifiée suivante est affichée.

   Lorsque la détection planifiée démarre, la colonne d'état pour les profils de détection sélectionnés indique En cours d'exécution, et la colonne Heure de la dernière exécution est mise à jour pour indiquer l'heure du début de la détection.

   Remarque : Pour déclencher la colonne Pourcentage d'avancement pendant que la détection s'exécute, cliquez sur Actualiser.

   Les unités détectées sont ajoutées à des collections d'unités, ce qui initialise la détection et l'interrogation des composants. La page Profil de détection s'affiche de nouveau.

   Si la détection se bloque pendant plus de 10 minutes, elle est interrompue. Une détection est considérée comme bloquée lorsqu'aucune nouvelle unité n'est détectée durant une période de 10 minutes *et* que l'état des profils de détection sélectionnés n'a pas changé depuis 10 minutes. Un événement d'audit est généré sur l'unité Data Aggregator.

   La colonne d'état des profils de détection sélectionnés indique Echec si aucune unité n'a été détectée, ou Echec partiel si au moins une unité a été détectée.

   La synchronisation avec CA Performance Center des composants surveillés et des unités détectées peut prendre jusqu'à 5 minutes. Lorsque la synchronisation est terminée, les unités détectées et les composants s'affichent dans l'onglet Inventaire de CA Performance Center.

5. (Facultatif) Pour synchroniser des unités détectées et des composants immédiatement avec CA Performance Center, procédez comme suit :

   a. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.

   b. Cliquez sur Data Aggregator dans le menu Statut du système.

   c. Sélectionnez Data Aggregator et cliquez sur le bouton Resynchroniser.

Affichage des résultats de la détection

Vous pouvez afficher un récapitulatif du nombre de nouvelles unités (ICMP) et gérables (SNMP) acceptant la commande ping qui ont été détectées pour une instance de détection spécifique. Vous pouvez également afficher les détails spécifiques concernant les unités détectées, notamment l'adresse IP, le modèle, le type, le nom de fournisseur, l'emplacement et les profils SNMP qui ont été utilisés.

Un résultat de détection peut également indiquer que les unités existantes ont été trouvées. Ce même profil ou un profil de détection différent a détecté les unités existantes préalablement. Pour afficher les unités existantes, utilisez le filtre Non modifié. Les unités existantes dont l'adresse IP est différente indiquent que les unités ont préalablement été détectées et sont surveillées avec une adresse IP différente.

Ce comportement est commun et attendu, car un nombre élevé d'unités peuvent répondre à plusieurs adresses IP. Data Aggregator gère l'ensemble complet d'adresses IP pour chaque unité et les ajoute toutes dans CA Performance Center.

Procédez comme suit :

1. Affichez la liste des profils de détection (page 68).
2. Sélectionnez un profil de détection pour lequel vous souhaitez afficher des résultats de détection et cliquez sur le bouton Historique.

   Remarque : Le bouton Historique est désactivé lorsque vous sélectionnez un profil de détection pour lequel aucune détection n'a été exécutée.
3. Sélectionnez une instance de détection, le cas échéant.
4. (Facultatif) Filtrez le tableau Unités détectées en effectuant l'une des opérations suivantes :

   - Filtrez par type d'unité en sélectionnant quels types d'unité vous voulez afficher à partir de la liste du filtre de type d'unité, cliquez sur Appliquer.
   - Filtrez en fonction de l'état des unités détectées en sélectionnant les états que vous souhaitez afficher dans la liste Etat et en cliquant sur Appliquer.
   - Filtrez par type d'unité et par état en faisant une sélection dans la liste de filtre de type d'unité et dans la liste Etat et en cliquant sur Appliquer.

   Les résultats de détection s'affichent dans le tableau Unités détectées. La colonne Profil SNMP indique le profil SNMP le plus élevé auquel l'unité a répondu.

   Plus précisément, la colonne Etat indique l'un des états suivants :

   Nouveau

   Indique une unité qui a été détectée pour la première fois lorsque ce profil de détection a été exécuté.

   Modifié

   Indique que le type d'une unité a changé depuis la détection précédente. Par exemple, une unité acceptant la commande ping et qui a été détectée préalablement est désormais détectée en tant qu'unité gérable, ou une unité préalablement gérable avec le type Commutateur est désormais identifiée avec le type Routeur, etc. Les unités affichant uniquement une modification d'attribut (nom d'hôte, description de système, etc.) n'apparaissent pas dans la liste Modifié.

Non modifié

Indique que les unités existantes n'ont pas été modifiées. Les unités existantes présentant uniquement une modification d'attribut apparaissent également dans la liste Non modifié.

Supprimé

Indique que l'unité a été supprimée de Data Aggregator suite à l'exécution d'une détection.

Remarque : Si une unité détectée individuelle n'est pas reconnue comme acceptant la commande ping ou comme gérable, son état est Inaccessible. Toutefois, Data Aggregator ne signale *pas* les unités inaccessibles qui sont trouvées dans une plage d'adresses IP.

Informations complémentaires :

Profils SNMP (page 62)
Flux de travaux de détection (page 60)

Détection à partir d'autres sources de données

Vous pouvez choisir la détection automatique de Data Aggregator des unités synchronisées avec CA Performance Center par d'autres sources de données. Cette option est disponible lorsque vous enregistrez Data Aggregator ou si vous modifiez des options de source de données. Cette option est désactivée par défaut.

Important : Lorsque cette option est activée, Data Aggregator tente de détecter les unités fournies par *toutes* les autres sources de données. Vous ne pouvez pas affiner cette fonction pour l'appliquer à un ensemble de sources de données particulier.

Lorsque cette option est activée, Data Aggregator tente de détecter toute nouvelle unité à partir de ce point. Pour que Data Aggregator tente de détecter des unités ayant déjà été synchronisées avec CA Performance Center, sélectionnez la source de données Data Aggregator, cliquez sur Resynchroniser et activez la case à cocher Effectuer une resynchronisation complète.

La tentative de détection produit une unité acceptant la commande ping ou d'un autre type dans Data Aggregator si l'unité est accessible via ICMP ou un autre protocole pris en charge.

Remarque : Si vous désactivez cette option à tout moment après son activation, Data Aggregator continue de surveiller les unités ayant déjà été détectées.

Pour activer cette option, cochez la case Détecter les unités d'autres sources de données située dans la boîte de dialogue Modifier la source des données sur la page Gérer les sources de données dans CA Performance Center.

Informations complémentaires :

Détection d'unités (page 59)

Modifications du type d'unité

En fonction des informations de service d'unité, Data Aggregator peut automatiquement classer les unités gérables comme Routeur, Commutateur et Serveur. Si une unité gérable n'est pas identifiable comme Routeur, Commutateur ou Serveur, elle est classée sous le type Unité.

Si les types de certaines unités gérables SNMP n'ont pas été identifiés comme vous l'espériez, vous pouvez corriger ces types. Mappez la valeur de base de données d'informations de gestion sysObjectID explicitement vers le type d'unité correct dans le fichier $KARAF_HOME/custom/devicetypes/DeviceTypes.xml qui est fourni avec Data Aggregator.

Remarque : Vous ne pouvez pas ajouter de nouveaux types d'unité au fichier DeviceTypes.xml.

Le fichier DeviceTypes.xml contient un modèle pour mapper l'élément sysObjectID avec les types d'unité appropriés. Par défaut, le fichier ne contient aucune entrée de mappage sysObjectID-to-type. Si vous voulez classer un type d'unité avec un ID sysObjectID particulier, vous pouvez modifier le modèle pour ajouter les entrées sysObjectID-to-type dans le fichier. Avant d'ajouter un ID sysObjectID, supprimez les marques de commentaire de la section dans laquelle vous ajoutez l'ID.

Remarque : Une minute est requise pour l'application des mises à jour du fichier DeviceTypes.xml.

Vous pouvez classer une unité dans plusieurs types d'unité. Toutefois, le type Unité est mutuellement exclusif des autres types d'unité. Par exemple, si vous ajoutez un ID sysObjectID à un ou plusieurs types d'unités Routeur, Commutateur ou Serveur et que vous ajoutez également cet ID au type d'unité Unité, ce dernier type est ignoré et n'est pas reconnu.

Remarque : Si vous mettez à niveau Data Aggregator, le fichier DeviceTypes.xml n'est pas conservé. Toutefois, les configurations ajoutées avant la mise à niveau *sont conservées.*

Exemple : Mappage d'un ID sysObjectID d'unité vers un autre type d'unité

Procédez comme suit :

1. Ouvrez le fichier $KARAF_HOME/custom/devicetypes/DeviceTypes.xml.

2. Entrez les informations suivantes :

```
<DeviceType>
    <Routers>
     <sysObjectID>1.3.6.5.1.34</sysObjectID>
    </Routers>

    <Switches>
      <sysObjectID>1.3.6.5.5.3</sysObjectID>
      <sysObjectID>1.3.6.5.1.34</sysObjectID>
     </Switches>

    <Servers>
      <sysObjectID>1.3.6.5.567.1</sysObjectID>
    </Servers>

    <Device>
      <sysObjectID>1.3.6.5.49.1</sysObjectID>
    </Device>
<DeviceType>
```

3. Exécutez la détection sur le profil de détection qui contient les unités.

   Remarque : Les modifications que vous apportez au fichier DeviceTypes.xml sont appliquées aux unités existantes lorsque vous exécutez de nouveau la détection.

   L'exécution de la détection entraîne les résultats suivants :

   - Toutes les unités qui ont un ID sysObjectID de 1.3.6.5.1.34 sont classées comme type d'unité Routeur et Commutateur.
   - Toutes les unités qui ont un ID sysObjectID de 1.3.6.5.5.3 sont classées comme type d'unité Commutateur.
   - Toutes les unités qui ont un ID sysObjectID de 1.3.6.5.567.1 sont classées comme type d'unité Serveur.
   - Toutes les unités qui ont un ID sysObjectID de 1.3.6.5.49.1 sont classées comme type d'unité Unité.

Nouvelle détection

Vous pouvez redétecter des unités surveillées existantes lorsqu'un profil de détection contenant l'une de leurs adresses IP ou noms d'hôte est exécuté. Pour redétecter une seule unité surveillée, cliquez sur Redétecter dans l'onglet Détails de l'unité.

Vous pouvez mettre l'ensemble suivant d'attributs à jour suite à cette détection :

- Nom de système
- Nom d'hôte
- Type d'unité (affichée dans CA Performance Center)
- Location (Emplacement)
- Fournisseur
- Description de l'unité
- Modèle d'unité

Remarque : Les modifications apportées aux attributs d'unité peuvent entraîner des modifications au niveau des groupes et des collections d'unités auxquels une unité appartient. Les modifications apportées aux groupes et aux collections d'unités peuvent entraîner l'ajout ou la suppression de profils de surveillance.

L'affichage des modifications au niveau des attributs d'unité dans l'inventaire ou les vues de tableaux de bord CA Performance Center peut prendre jusqu'à 5 minutes.

Chapitre 4: Gestion de l'infrastructure

Ce chapitre traite des sujets suivants :

Personnalisation du flux de travaux de gestion des unités et des composants (page 85)
Profils de surveillance (page 88)
Collections d'unités prédéfinies (page 93)
Collections d'unités personnalisées (page 98)
Affichage des unités surveillées (page 99)
Suppression d'unités (page 102)
Modification de l'adresse IP principale d'une unité surveillée (page 103)
Suppression des composants retirés (page 103)
Suppressions de domaine IP (page 106)
Suppressions de client hébergé (page 107)
Désactivation des clients hébergés (page 107)
Activation des clients hébergés (page 109)
Reconfiguration des unités (page 110)

Personnalisation du flux de travaux de gestion des unités et des composants

Vous pouvez personnaliser la gestion des unités détectées et des composants surveillés. Les options incluent la modification des profils et des associations, la création de certifications de fournisseur et l'importation de familles de mesures. Par exemple, vous pouvez interroger des interfaces critiques plus fréquemment ou appliquer des profils de surveillance personnalisés avec des règles d'événement à des collections d'unités personnalisées.

Le flux de travaux suivant constitue une méthode rapide de personnalisation.

Connectez-vous en tant qu'utilisateur avec le rôle Administrateur et effectuez les étapes suivantes :

1. Créez de nouveaux profils de surveillance (ou faites des copies des profils de surveillance prédéfinis) afin de personnaliser les taux d'interrogation et les mesures pour la surveillance de vos unités.
2. (Facultatif) Ajoutez des règles d'événement à des profils de surveillance personnalisés (page 144).

3. (Facultatif) Si les certifications de fournisseur prédéfinies et les familles de mesures associées ne satisfont pas vos besoins, créez des certifications de fournisseur personnalisées et importez des nouvelles familles de mesures. Cela peut se faire à tout moment.

   Remarque : Pour plus d'informations sur les familles de mesures personnalisées et les certifications de fournisseur personnalisées, reportez-vous au *Manuel d'autocertification de Data Aggregator*.

4. Créez des collections d'unités personnalisées et des règles associées dans CA Performance Center ; elles seront ensuite utilisées comme collections d'unités Data Aggregator. Vous pouvez synchroniser ces collections avec Data Aggregator immédiatement ou attendre que la synchronisation automatique ait lieu. Vous pouvez ajouter manuellement les unités dans ces collections après la détection.

   Remarque : Si vous êtes un MSP ou un client hébergé, effectuez cette étape en tant qu'administrateur de clients hébergés. Pour plus d'informations sur la création des groupes surveillés et sur la synchronisation des sources de données, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

5. Personnalisez votre profil de surveillance et vos associations de collection d'unités pour vous assurer que le taux d'interrogation souhaité est utilisé (page 92). Lorsque vous créez un profil de surveillance personnalisé, associez-le à une collection d'unités personnalisée pour l'activer, ainsi que toutes les règles d'événement associées.

   Remarque : Si vous êtes un MSP ou un client hébergé, effectuez cette étape en tant qu'administrateur de clients hébergés.

   La personnalisation peut inclure la suppression d'associations entre des profils de surveillance prédéfinis et des collections d'unités, ainsi que l'association de profils de surveillance personnalisés à des collections d'unités prédéfinies ou personnalisées.

6. Révisez les résultats de la surveillance de composants une fois que le processus d'interrogation avec la nouvelle configuration a commencé à vérifier que vous collectez les informations appropriées (page 99).

   Remarque : Si vous êtes un MSP ou un client hébergé, effectuez cette étape en tant qu'administrateur de clients hébergés.

Diagramme illustrant le flux de travaux d'une entreprise :

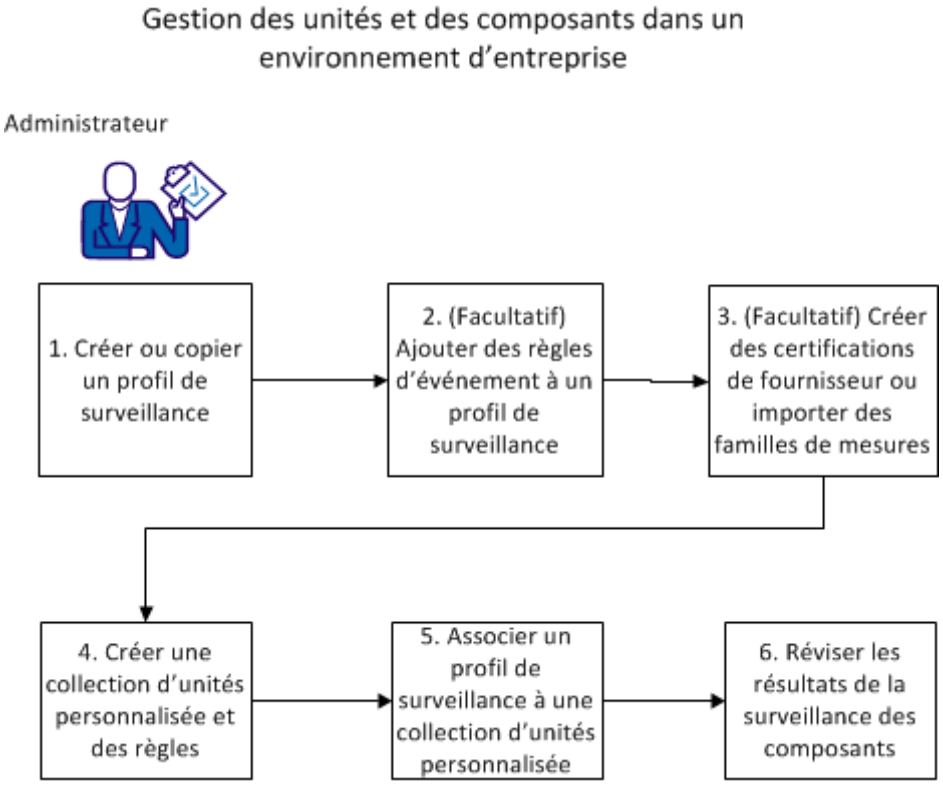
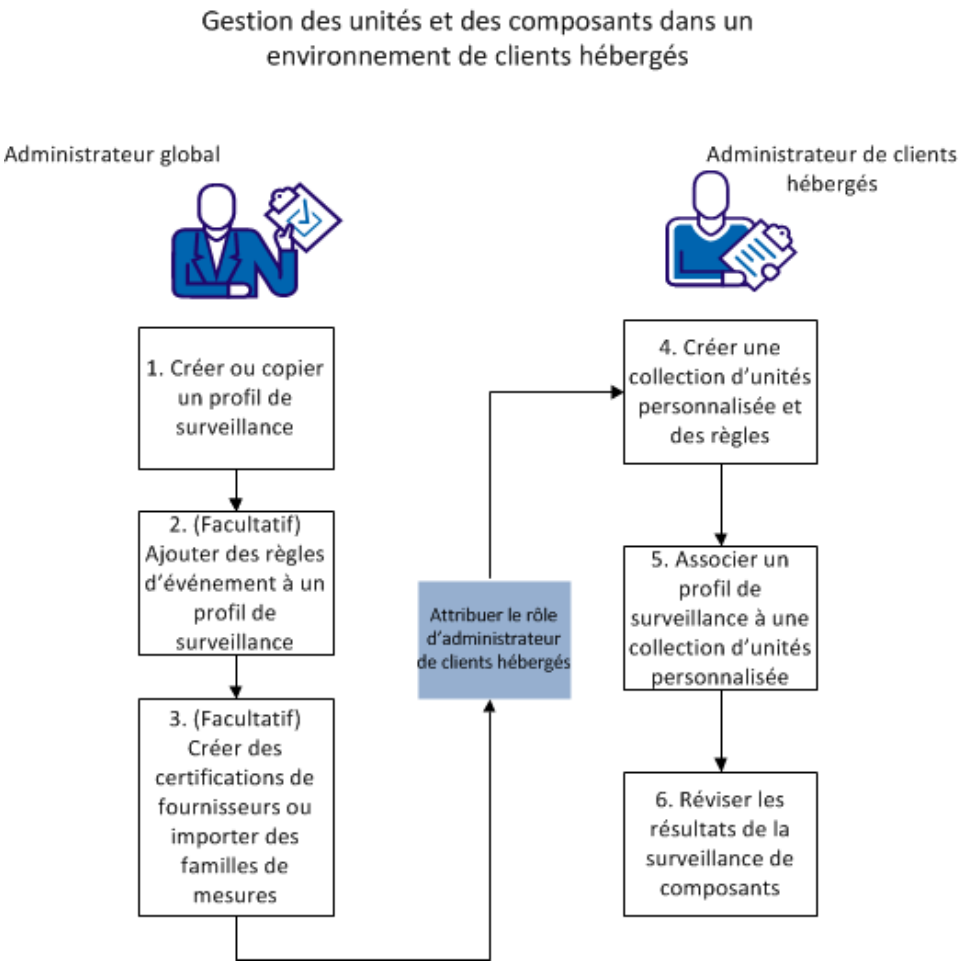


Diagramme illustrant le flux de travaux d'un environnement de client hébergé :



Profils de surveillance

Les profils de surveillance déterminent la vitesse d'interrogation et les statistiques qui sont détectées et interrogées pour les unités d'une collection. Une sélection de profils de surveillance prédéfinis (prêts à l'emploi) est fournie. Les profils de surveillance prédéfinis sont automatiquement appliqués à des collections d'unités prédéfinies, comme la collection All Routers (Tous les routeurs). Vous ne pouvez pas modifier les profils de surveillance prédéfinis ou les supprimer du système, mais vous pouvez les supprimer d'une collection d'unités ou les copier pour créer un profil personnalisé.

Vous pouvez créer, modifier, copier ou supprimer des profils de surveillance personnalisés en vous connectant en tant qu'administrateur. Les profils de surveillance personnalisés sont mis à disposition globalement dans l'interface utilisateur et ne sont pas limités aux clients hébergés, même si vous êtes un administrateur de MSP travaillant dans un espace de travail de client hébergé. (Toutefois, les collections d'unités auxquelles les profils de surveillance sont associés sont limitées aux clients hébergés). Par exemple, vous pouvez créer un profil "Surveillance de routeur de service Or" et l'utiliser pour tous vos clients hébergés de niveau or. Vous ne devez pas créer un profil "Surveillance de routeur de service Or" *distinct* pour *chaque* client hébergé de niveau or.

L'unicité du nom des profils de surveillance est appliquée à l'ensemble des clients hébergés.

Utilisez l'interface utilisateur de CA Performance Center ou les services Web REST de Data Aggregator pour gérer les profils de surveillance et afficher leurs associations avec les collections d'unités.

Associations de profils de surveillance prédéfinis

Les profils de surveillance spécifient les statistiques à interroger. Les profils de surveillance prédéfinis (prêts à l'emploi) sont automatiquement associés à des collections d'unités, comme suit :

- Le profil de surveillance Accessibilité est associé à la collection d'unités All Devices (Toutes les unités).
- Le profil de surveillance Accessibilité est associé à la collection d'unités All Devices (Toutes les unités).
- Le profil de surveillance Routeur est associé à la collection d'unités All Routers (Tous les routeurs).
- Le profil de surveillance Serveur physique est associé à la collection d'unités All Servers (Tous les serveurs).
- Le profil de surveillance Serveur virtuel est associé à la collection d'unités All Servers (Tous les serveurs).
- Le profil de surveillance Commutateur est associé à la collection d'unités All Switches (Tous les commutateurs).
- Le profil de surveillance Microsoft Cluster Services est associé à la collection d'unités All Servers (Tous les serveurs).
- Le profil de surveillance VMware est associé à la collection d'unités All VMware vCenters (Tous les serveurs VMware vCenter).

- Le profil de surveillance Hôte VMware ESX est associé à la collection d'unités All VMware vCenters (Tous les serveurs VMware vCenter).
- Le profil de surveillance Machine virtuelle VMware est associé à la collection d'unités All VMware vCenters (Tous les serveurs VMware vCenter).

Les profils de surveillance suivants n'ont pas d'associations prédéfinies à des collections d'unités. Cette conception empêche des détections de grande ampleur qui peuvent nuire aux performances. Pour collecter des données, affectez manuellement ces profils de surveillance à des collections d'unités :

- Interface réseau
- Chemin de réponse
- MPLS
- CBQoS

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Collection d'unités All Devices (Toutes les unités) (page 95)
Collection d'unités All Routers (Tous les routeurs) (page 95)
Assignation ou suppression des profils de surveillance des collections d'unités (page 92)

Affichage des profils de surveillance

Les administrateurs peuvent afficher une liste des profils de surveillance et leurs associations aux collections d'unités.

- Ils peuvent afficher les collections d'unités associées au client hébergé qu'ils administrent.
- Un administrateur de clients hébergés peut afficher sa propre liste de collections d'unités.

Ces informations permettent de déterminer la méthode à utiliser pour gérer vos profils de surveillance et les fréquences d'interrogation, et donnent une idée des types de rapport que vous pouvez générer pour une collection d'unités.

Procédez comme suit :

1. Cliquez sur Profils de surveillance dans le menu Configuration de la surveillance pour une source de données de Data Aggregator.

   Une liste de profils de surveillance est remplie.

2. Vous pouvez ajouter un profil de surveillance au système ou sélectionner un profil de surveillance à modifier, à copier ou à supprimer si vous êtes un administrateur. Tous les profils de surveillance, y compris les profils personnalisés, sont globaux.

   Remarque : Vous ne pouvez pas modifier de profils de surveillance prédéfinis ou les supprimer ; seuls les profils de surveillance personnalisés sont modifiables.

3. Sélectionnez un profil de surveillance.

4. Les détails du profil de surveillance sélectionné remplissent les onglets, comme suit :

   - L'onglet Familles de mesures reprend une liste des familles de mesures associées à ce profil de surveillance spécifique. Les familles de mesures contiennent les mesures qui sont utilisées pour interroger les unités et les interfaces.
   - L'onglet Règles d'événement reprend une liste des règles d'événement associées à ce profil de surveillance spécifique. En tant qu'administrateur, vous pouvez gérer les relations entre les règles d'événement et le profil de surveillance sélectionné en affectant ou en supprimant des règles.
   - L'onglet Collections reprend la liste des collections d'unités qui sont associées à ce profil de surveillance. En tant qu'administrateur de clients hébergés, vous pouvez gérer les relations entre une collection d'unités et le profil de surveillance sélectionné en affectant ou en supprimant des profils.

Informations complémentaires :

Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Mise à jour automatique de la reconfiguration des unités (page 113)

Assignation ou suppression des profils de surveillance des collections d'unités

Les administrateurs ou les administrateurs de clients hébergés peuvent ajouter ou supprimer une relation entre une collection d'unités spécifique et les profils de surveillance dans le système. Cette capacité vous permet de démarrer ou d'arrêter l'interrogation des statistiques associées à un profil de surveillance par rapport aux unités et aux composants d'une collection d'unités.

Important : Lorsque vous assignez des profils de surveillance à des collections d'unités, des demandes SNMP peuvent se produire. Ces demandes peuvent affecter les performances de l'unité. De plus, n'associez pas de profils de surveillance à la collection d'unités All Devices (Toutes les unités), car des demandes SNMP supplémentaires pourraient être envoyées aux demandes acceptant uniquement la commande ping, ce qui pourrait entraîner la prise en charge sporadique des familles de mesures.

Par exemple, vous disposez d'un routeur détecté avec 1 000 interfaces physiques et logiques. Vous avez également créé un profil de surveillance d'interface et vous avez défini le taux d'interrogation sur ce profil de surveillance sur une minute. Si le profil de surveillance d'interface est assigné à la collection d'unités dans laquelle se trouve le routeur, dix objets MIB seront interrogés pour chaque interface. Ce qui entraîne un taux de 166 objets MIB par seconde pour l'agent SNMP auxquels vous devez répondre. Cette importante charge SNMP peut affecter les performances du routeur.

Les familles de mesures telles que la qualité de service, MPLS et IPSLA peuvent également contribuer à des demandes SNMP significatives. Pour plus d'informations sur les implications et les restrictions des demandes SNMP à vos périphériques réseau, consultez les manuels du fournisseur ou contactez le fournisseur.

Remarque : Data Aggregator utilise le taux d'interrogation le plus rapide qui est configuré lorsque plusieurs collections d'unités sont affectées à un profil de surveillance. Supprimez les associations de profils de surveillance prédéfinis avec les collections d'unités lorsque vous voulez utiliser votre taux d'interrogation personnalisé.

Procédez comme suit :

1. Cliquez sur Collections dans le menu Configuration de la surveillance pour consulter une source de données Data Aggregator.

   Une liste de collections s'affiche. Ils peuvent afficher les collections d'unités associées au client hébergé qu'ils administrent. Un administrateur de clients hébergés peut afficher sa propre liste (client hébergé) de collections d'unités.

2. Sélectionnez une collection et cliquez sur l'onglet Profils de surveillance.

   Une liste affiche les profils de surveillance qui sont assignés à la collection d'unités sélectionnée.

3. Cliquez sur Gérer.

   La boîte de dialogue Assigner des profils de surveillance de collection s'ouvre.

4. Effectuez l'une des actions suivantes :
   - Sélectionnez un ou plusieurs profils de surveillance dans la liste Profils de surveillance disponibles, puis cliquez sur Ajouter.

     Les profils de surveillance sélectionnés passent dans la liste Profils de surveillance assignés.

     L'association d'un profil de surveillance à une collection d'unités active les règles d'événement incluses dans le profil de surveillance. Les événements sont générés et effacés lorsque les unités de la collection d'unités remplissent les conditions de règle d'événement.
   - Sélectionnez un ou plusieurs profils de surveillance dans la liste Profils de surveillance assignés, puis cliquez sur Supprimer.

     Les profils de surveillance sélectionnés passent dans la liste Profils de surveillance disponibles.

     Remarque : La suppression de la relation ne supprime pas les profils de surveillance du système.
5. Cliquez sur Enregistrer.

   Vos modifications sont enregistrées et peuvent être vérifiées en répétant l'étape 2.

Informations complémentaires :

Associations de profils de surveillance prédéfinis (page 89)
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Personnalisation du flux de travaux de gestion des unités et des composants (page 85)
Méthode de définition et d'activation d'un filtre d'interface (page 129)

Collections d'unités prédéfinies

Data Aggregator et CA Performance Center prennent en charge le concept de *collections d'unités*, qui sont des groupements logiques d'unités surveillées.

Plusieurs collections d'unités prédéfinies (prêtes à l'emploi) sont fournies pour obtenir des données dans votre système Data Aggregator rapidement et pour tester le produit. Les unités qui sont détectées pendant la détection sont ajoutées à ces collections en fonction de leur type. Par exemple, les routeurs sont ajoutés à la collection d'unités prédéfinie All Routers (Tous les routeurs). Lors de la synchronisation, ces unités surveillées sont ajoutées aux collections correspondantes dans CA Performance Center.

Les profils de surveillance prédéfinis sont alors automatiquement appliqués aux collections d'unités prédéfinies, ce qui permet de collecter immédiatement les données, sans intervention de votre part. Une fois que ces données ont été collectées, vous pouvez exécuter des rapports sur les données pour mieux comprendre votre réseau.

Les collections d'unités prédéfinies suivantes sont fournies :

- All Devices (Toutes les unités) (page 95)
- All Routers (Tous les routeurs) (page 95)
- All Servers (Tous les serveurs) (page 95)
- All Switches (Tous les commutateurs) (page 96)
- All Manageable Devices (Toutes les unités gérables) (page 96)
- All ESX Hosts (Tous les hôtes ESX) (page 97)
- All Virtual Machines (Tous les ordinateurs virtuels) (page 97)
- All VMware vCenters (Tous les serveurs VMware vCenter) (page 97)

Remarque : Les collections d'unités prédéfinies sont principalement destinées à une utilisation de type labo ou en mode démonstration. Dans un déploiement de production réel, il est recommandé de concevoir et de configurer des collections d'unités personnalisées pour permettre un contrôle détaillé et une collecte de données optimale.

Accédez au menu Configuration de la surveillance pour afficher une liste de collections d'unités et les profils de surveillance qui sont appliqués à chacune. Les administrateurs peuvent afficher les collections d'unités associées au client hébergé qu'ils administrent. Un administrateur de clients hébergés peut afficher sa propre liste de collections d'unités.

Informations complémentaires :

Associations de profils de surveillance prédéfinis (page 89)
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Collections d'unités personnalisées (page 98)

Collection d'unités All Devices (Toutes les unités)

La collection d'unités All Devices (Toutes les unités) est une collection d'unités prédéfinie. Les unités gérables et acceptant la commande ping qui sont détectées pendant une détection sont automatiquement placées dans la collection d'unités All Devices (Toutes les unités). Les unités inaccessibles ne sont pas incluses dans cette collection.

Important : N'associez pas de profils de surveillance à la collection d'unités All Devices (Toutes les unités), car des demandes SNMP supplémentaires pourraient être envoyées aux demandes acceptant uniquement la commande ping, ce qui pourrait entraîner la prise en charge sporadique des familles de mesures.

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Associations de profils de surveillance prédéfinis (page 89)

Collection d'unités All Routers (Tous les routeurs)

La collection d'unités All Routers (Tous les routeurs) est une collection d'unités prédéfinie. Les routeurs détectés au cours d'une détection sont automatiquement placés dans la collection d'unités All Routers (Tous les routeurs).

Remarque : Les routeurs peuvent apparaître simultanément dans les collections d'unités All Routers (Tous les routeurs) et All Switches (Tous les commutateurs).

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Associations de profils de surveillance prédéfinis (page 89)

Collection d'unités All Servers (Tous les serveurs)

La collection d'unités All Servers (Tous les serveurs) est une collection d'unités prédéfinie. Les serveurs physiques et virtuels (hôtes) détectés sont automatiquement placés dans la collection d'unités All Servers (Tous les serveurs). Les unités réseau, telles que les routeurs et les commutateurs, ne sont pas incluses dans cette collection d'unités.

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Associations de profils de surveillance prédéfinis (page 89)

Collection d'unités All Switches (Tous les commutateurs)

La collection d'unités All Switches (Tous les commutateurs) est une collection d'unités prédéfinie. Les commutateurs détectés sont automatiquement placés dans la collection d'unités All Switches (Tous les commutateurs).

Remarque : Les commutateurs peuvent apparaître simultanément dans les collections d'unités All Routers (Tous les routeurs) et All Switches (Tous les commutateurs).

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Associations de profils de surveillance prédéfinis (page 89)

Collection d'unités All Manageable Devices (Toutes les unités gérables)

La collection d'unités All Manageable Devices (Toutes les unités gérables) est une collection prédéfinie. Les unités gérables collectent des statistiques de performances avancées et sont surveillées avec un protocole comme SNMP. Les unités gérables qui sont détectées pendant une détection sont automatiquement placées dans la collection d'unités All Manageable Devices (Toutes les unités gérables).

Les unités acceptant la commande ping peuvent être surveillées uniquement pour la disponibilité et ne fournissent pas de mesures de performances supplémentaires. Ces unités ne sont donc pas incluses dans la collection d'unités All Manageable Devices (Toutes les unités gérables).

Remarque : Les unités gérables peuvent s'afficher dans la collection d'unités All Devices (Toutes les unités) et dans la collection d'unités All Manageable Devices (Toutes les unités gérables).

Informations complémentaires :

Collections d'unités prédéfinies (page 93)

Collection d'unités All ESX Hosts (Tous les hôtes ESX)

La collection d'unités All ESX Hosts (Tous les hôtes ESX) est une collection d'unités prédéfinie. Les hôtes ESX détectés sont automatiquement placés dans la collection d'unités All ESX Hosts.

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Associations de profils de surveillance prédéfinis (page 89)

Collection d'unités All Virtual Machines (Toutes les machines virtuelles)

La collection d'unités All Virtual Machines (Toutes les machines virtuelles) est une collection d'unités prédéfinie. Les machines virtuelles VMware détectées sont automatiquement placées dans la collection d'unités All Virtual Machines.

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Associations de profils de surveillance prédéfinis (page 89)

Collection d'unités All VMware vCenters (Tous les serveurs VMware vCenters)

La collection d'unités All VMware vCenters (Tous les serveurs VMware vCenters) est une collection d'unités prédéfinie. Tous les serveurs qui exécutent systemEdge avec le module VCAIM et qui sont détectés sont automatiquement placés dans la collection d'unités All VMware vCenters.

Informations complémentaires :

Collections d'unités prédéfinies (page 93)
Associations de profils de surveillance prédéfinis (page 89)

Collections d'unités personnalisées

Les collections d'unités prédéfinies sont principalement destinées à une utilisation de type labo ou en mode démonstration. Dans un déploiement de production réel, il est recommandé de concevoir et de configurer des collections d'unités personnalisées pour permettre un contrôle détaillé des données interrogées. Par exemple, désactivez l'interrogation d'une unité en dissociant l'unité à partir d'une autre collection d'unités à laquelle des profils de surveillance sont associés. Si vous associez des profils de surveillance aux collections d'unités prédéfinies (All Routers (Tous les routeurs), par exemple), vous ne pouvez pas empêcher l'interrogation d'une unité unique. Pour désactiver l'interrogation, vous devez dissocier les profils de surveillance, car les unités des collections prédéfinies ne peuvent pas être supprimées. Vous devez ensuite créer des collections d'unités personnalisées qui contiennent des unités auxquelles vous voulez appliquer la même stratégie d'interrogation. Associez des profils de surveillance (ou profils de surveillance personnalisés) à ces collections d'unités personnalisées pour lancer l'interrogation.

Créez des collections d'unités personnalisées dans CA Performance Center, puis synchronisez-les immédiatement avec Data Aggregator ou attendez que la synchronisation se lance automatiquement. Au moment de la synchronisation, Data Aggregator crée les collections d'unités correspondantes à utiliser dans les unités de surveillance.

Remarque : Pour plus d'informations sur la création de collections d'unités personnalisées et leur synchronisation avec Data Aggregator, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

Accédez au menu Configuration de la surveillance pour afficher une liste de collections d'unités et les profils de surveillance qui sont appliqués à chacune. Les administrateurs peuvent afficher les collections d'unités associées au client hébergé qu'ils administrent. Un administrateur de clients hébergés peut afficher sa propre liste de collections d'unités.

Informations complémentaires :

Collections d'unités prédéfinies (page 93)

Affichage des unités surveillées

Vous pouvez afficher les détails des unités surveillées et leurs associations avec des collections d'unités, des composants, des profils de surveillance et des mesures. Vous pouvez également afficher un rapport de filtrage. Certaines informations seront disponibles en contexte, par exemple pour identifier les profils de surveillance utilisés pour interroger des composants d'unité.

Remarque : Certaines fonctionnalités requièrent des droits d'administrateur.

Les unités surveillées sont des unités gérables et des unités qui acceptent la commande ping (accessibles mais non gérables). Les unités inaccessibles ne sont pas des unités surveillées. Vous pouvez afficher les composants des unités surveillées à partir de l'onglet Familles de mesures interrogées.

Procédez comme suit :

1. Cliquez sur Unités surveillées dans le menu Inventaire surveillé d'une source de données de Data Aggregator.

   L'onglet Arborescence s'affiche.

2. Sélectionnez Unité par collection ou Unité par profil de surveillance dans la liste déroulante, puis sélectionnez une unité spécifique dans l'arborescence correspondante.

   Remarque : Vous pouvez aussi sélectionner l'onglet Recherche pour effectuer une recherche par nom d'hôte, nom d'unité ou adresse IP. Vous pouvez entrer un nom ou une adresse IP partielle pour renvoyer une liste d'unités qui contiennent cette correspondance partielle. Les caractères génériques et les expressions régulières ne sont pas pris en charge.

   L'onglet Détails fournit des informations sur l'unité surveillée sélectionnée. Ces informations comprennent notamment l'adresse IP de l'unité, le profil SNMP associé, le statut de l'unité, etc. Vous pouvez modifier l'adresse IP, l'hôte Data Collector, le profil SNMP et la version SNMP de l'unité.

   Vous pouvez modifier l'adresse IP de l'unité de deux façons :

   - Modifiez le champ Adresse IP, puis cliquez sur Enregistrer.
   - Cliquez avec le bouton droit de la souris sur une adresse IP dans la table Adresses IP, sélectionnez l'option Définir cette adresse IP comme adresse IP principale de l'unité, puis cliquez sur Enregistrer.

   Remarque : Des informations supplémentaires sont disponibles dans cette vue pour les unités gérables.

(Facultatif) Cliquez sur Redétecter pour redétecter l'unité. Vous pouvez mettre l'ensemble suivant d'attributs à jour suite à cette détection :

- Nom du système
- Nom d'hôte
- Type d'unité (affiché dans CA Performance Center)
- Emplacement
- Fournisseur
- Description de l'unité
- Modèle d'unité

Remarque : Les modifications apportées aux attributs d'unité peuvent entraîner des modifications au niveau des groupes et des collections d'unités auxquels une unité appartient. Les modifications apportées aux groupes et aux collections d'unités peuvent entraîner l'ajout ou la suppression de profils de surveillance.

Vérifiez que l'unité a été redétectée en recherchant l'événement que la nouvelle détection a déclenché. Pour afficher des événements, cliquer sur le menu Tableaux de bord dans CA Performance Center et, sous Affichages des opérations, sélectionnez Affichage des événements.

3. (Facultatif) Sélectionnez une famille de mesures et cliquez sur Mettre à jour la famille de mesures pour reconfigurer des composants pour les mises à jour de configuration. Par exemple, si vous ajoutez un lecteur de disque sur un serveur, vous pouvez utiliser le bouton Mettre à jour la famille de mesures pour redétecter la mise à jour de configuration. La mise à jour de configuration crée un composant de disque.
4. Sélectionnez un autre onglet :
   - L'onglet Familles de mesures interrogées indique l'ensemble total de familles de mesures qui doivent être interrogées au niveau d'une unité ainsi que leurs fréquences d'interrogation. Cet ensemble total est basé sur la consolidation de tous les profils de surveillance définis pour l'unité. Cet onglet indique également si l'unité prend en charge les différentes familles de mesures.

     Le tableau Composants pour une famille de mesures donnée affiche le statut d'interrogation des composants pour un composant de famille de mesures qui a préalablement été détecté. L'un des éléments suivants s'affiche dans la colonne Statut :

     Actif

     Indique que le composant est en cours d'interrogation.

     Inactive

     Indique que l'interrogation sur le composant est arrêtée, car la famille de mesures n'est plus surveillée pour l'unité.

Retiré

Indique que le composant n'existe plus sur l'unité physique. L'interrogation sur le composant est arrêtée. Vous pouvez afficher des données historiques à des fins de génération de rapports. Par défaut, les composants retirés ne sont pas synchronisés avec CA Performance Center. Pour activer cette option, cochez la case Synchroniser les éléments retirés dans la boîte de dialogue Modifier la source des données de la page Gérer les sources de données de CA Performance Center.

(Facultatif) Sélectionnez une famille de mesures et cliquez sur Mettre à jour la famille de mesures pour reconfigurer des composants pour les mises à jour de configuration. Par exemple, si vous ajoutez un lecteur de disque sur un serveur, vous pouvez utiliser le bouton Mettre à jour la famille de mesures pour redétecter la mise à jour de configuration. La mise à jour de configuration crée un composant de disque.

- L'onglet Profils de surveillance permet de sélectionner une collection d'unités pour consulter les noms de profils associés. Placez le curseur sur un profil pour afficher sa description.
- L'onglet Mesures est rempli d'une liste de mesures prises en charge par cette unité. Sélectionnez une famille de mesures pour afficher ses détails. Affichez la certification de fournisseur d'implémentation, la source de fournisseur (la source du tableau MIB s'affiche s'il s'agit d'une certification de fournisseur SNMP) et l'expression utilisée pour calculer chaque mesure.
- L'onglet Rapport de filtrage indique les critères de filtrage de l'interface qui ont été utilisés pendant la surveillance du composant. L'onglet présente également un rapport de toutes les interfaces identifiées sur l'unité et indique si elles correspondent aux critères de filtrage spécifiés. Si vous modifiez les règles sur un profil de surveillance personnalisé, le volet de Critères de filtrage de l'interface ne reflète pas ces modifications. Si vous dissociez le profil de surveillance d'un groupe, le volet Critères de filtrage de l'interface ne reflète pas ces modifications. Redétectez l'unité pour filtrer les interfaces qui sont basées sur les modifications que vous avez apportées aux critères de filtrage et au profil de surveillance.

Informations complémentaires :

Détection et interrogation (page 63)
Mise à jour manuelle de la reconfiguration des unités (page 114)
Suppression d'un filtre d'interface (page 131)
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Méthode de définition et d'activation d'un filtre d'interface (page 129)

Suppression d'unités

Vous pouvez supprimer des unités détectées. Par exemple, vous pouvez supprimer une unité détectée si vous souhaitez cesser de la surveiller.

Lorsque vous supprimez une unité, vous obtenez les résultats suivants :

- Tous les composants de l'unité associée sont supprimés.
- Les données historiques sur les unités supprimées et les composants des unités ne sont plus accessibles.

Remarque : Si l'un des profils de détection de la liste est réexécuté, vous pouvez détecter à nouveau les unités supprimées.

Procédez comme suit :

1. Cliquez sur Unités surveillées dans le menu Inventaire surveillé d'une source de données de Data Aggregator.

   L'onglet Arborescence s'affiche.

2. Sélectionnez l'onglet Recherche avancée.

   Remarque : N'utilisez pas la zone de recherche globale en haut de la page.

3. Pour rechercher l'unité surveillée à supprimer, entrez le texte approprié dans la zone de recherche locale. Vous pouvez effectuer une recherche par nom d'hôte, par nom d'unité ou par adresse IP. Vous pouvez entrer un nom ou une adresse IP partielle pour renvoyer une liste d'unités qui contiennent cette correspondance partielle.

   Remarque : Les caractères génériques et les expressions régulières ne sont pas pris en charge.

   Une liste d'unités correspondantes est renvoyée.

4. Effectuez l'une des opérations suivantes :

   - Sélectionnez un ou plusieurs unités à supprimer et cliquez sur Supprimer.
   - Pour supprimer *toutes* les unités dans la liste de résultats, cochez la case qui s'affiche à côté de la colonne Nom et cliquez sur Supprimer.

   Une boîte de dialogue de confirmation s'ouvre.

5. Cliquez sur Oui pour confirmer la suppression.

   Les unités sont supprimées et ne sont plus visibles dans l'inventaire d'unités surveillées. Si une autre source de données ne gère pas ces unités, ces dernières ne s'afficheront plus dans la vue Inventaire, ni en tant que membres de groupes la prochaine fois que Data Aggregator se synchronise avec CA Performance Center.

Modification de l'adresse IP principale d'une unité surveillée

Vous pouvez modifier l'adresse IP principale d'une unité surveillée.

Procédez comme suit :

1. Cliquez sur Unités surveillées dans le menu Inventaire surveillé d'une source de données de Data Aggregator.

   L'onglet Arborescence s'affiche.

2. Sélectionnez Unité par collection ou Unité par profil de surveillance dans la liste déroulante, puis sélectionnez une unité spécifique dans l'arborescence correspondante.

   Remarque : Vous pouvez aussi sélectionner l'onglet Recherche pour effectuer une recherche par nom d'hôte, nom d'unité ou adresse IP. Vous pouvez entrer un nom ou une adresse IP partielle pour renvoyer une liste d'unités qui contiennent cette correspondance partielle. Les caractères génériques et les expressions régulières ne sont pas pris en charge.

3. Modifiez l'adresse IP principale en effectuant l'une des opérations suivantes :

   - Modifiez le champ Adresse IP, puis cliquez sur Enregistrer.
   - Cliquez avec le bouton droit de la souris sur une adresse IP dans la table Adresses IP, sélectionnez l'option Définir cette adresse IP comme adresse IP principale de l'unité, puis cliquez sur Enregistrer.

   Vous avez modifié l'adresse IP principale.

Suppression des composants retirés

Data Aggregator inclut un script permettant de supprimer les composants retirés. Une fois retirés les composants ne sont plus présents sur aucune unité physique. La présence de nombres excessifs de composants retirés peut affecter les performances de l'interface utilisateur. Pour supprimer des composants retirés, vous devez comprendre le fonctionnement de ce script.

Remarque : Pour connaître la procédure à suivre pour automatiser la suppression des composants retirés, consultez le *Manuel d'administration à l'aide des services Web REST de Data Aggregator*.

Procédez comme suit :

1. Ouvrez une invite de commande et accédez au répertoire /opt/IMDataAggregator/scripts.
2. Pour appeler le script de suppression des composants retirés, saisissez la commande suivante :

   ```
   ./remove_retired_items.sh
   ```

   Les paramètres de script sont affichés dans une liste et décrits.

Exemple : renvoi du nombre total de composants retirés

1. Saisissez la commande suivante :

   ```
   ./remove_retired_items.sh -h nom_hôte
   ```

   -h *nom_hôte*

   Spécifie le nom d'hôte Data Aggregator auquel la connexion doit être établie.

   Le nombre total de composants retirés s'affiche.
2. (Facultatif) Entrez le chiffre 1 pour renvoyer la liste des *noms* des composants retirés.
3. (Facultatif) Entrez le chiffre 1 pour supprimer tous les composants retirés.

Exemple : filtrage de la liste de composants retirés en fonction d'un critère spécifique

1. Pour appeler le script de suppression des composants retirés, saisissez la commande suivante :

   ```
   ./remove_retired_items.sh
   ```

   Les paramètres de script sont affichés dans une liste et décrits.
2. Supprimez les composants retirés en fonction d'un critère spécifique :
   - Si plusieurs instances de Data Collector sont installées, des adresses IP peuvent être dupliquées. Pour filtrer les composants retirés par adresse IP, procédez comme suit :
     a. Saisissez la commande suivante :

        ```
        ./remove_retired_items.sh -h nom_hôte -a adresse_IP_unité
        ```

     b. **Remarque :** La saisie d'une plage d'adresses IP n'est pas prise en charge.

     c. (Facultatif) Entrez le chiffre 1 pour renvoyer la liste des *noms* des composants retirés.

     d. (Facultatif) Entrez le chiffre 1 pour supprimer tous les composants retirés.
   - Pour supprimer des composants retirés en fonction de leur ancienneté (en nombre de jours d'ancienneté), saisissez la commande suivante :

     ```
     ./remove_retired_items.sh -h nom_hôte -t jours_écoulés
     ```

Par exemple, la commande ci-dessous supprime les composants retirés au cours des dix derniers jours :

```
./remove_retired_items.sh -h nom_hôte -t 10
```

Exemple : suppression d'un nombre élevé de composants retirés

Vous pouvez facilement supprimer tous les composants retirés dont le nombre total est supérieur à 100 000 :

- Pour examiner tous les composants retirés lorsque leur nombre total est supérieur à 100 000, saisissez la commande suivante :

  ```
  ./remove_retired_items.sh -h nom_hôte –o fichier_sortie
  ```

  -o *fichier_sortie*

  Correspond à la sortie de tous les composants retirés. Cette sortie prend la forme d'un fichier CSV.

  Par exemple, la commande suivante affiche la liste de tous les composants retirés. Le format de fichier CSV inclut l'ID d'élément de l'unité, le nom d'affichage de l'unité ainsi que l'ID et le nom d'affichage du composant retiré :

  ```
  ./remove_retired_items.sh -h my_host_name –o myretired.csv
  ```

- Pour supprimer la totalité des composants retirés lorsque leur nombre total est supérieur à 100 000 et journaliser les informations dans un fichier CSV, saisissez la commande suivante :

  ```
  ./remove_retired_items.sh -h nom_hôte –o fichier_sortie –c Yes
  ```

  -o *fichier_sortie*

  Correspond à la sortie de tous les composants retirés. Cette sortie prend la forme d'un fichier CSV.

  –c Yes

  Confirme la suppression de tous les composants retirés.

  Par exemple, la commande suivante supprime tous les composants retirés :

  ```
  ./remove_retired_items.sh -h my_host_name –o myretired.csv –c Yes
  ```

Tenez compte des autres aspects ci-dessous en matière de suppression des composants retirés :

- Si vous filtrez les composants retirés par nom de domaine IP ou par ID de domaine IP, vous devez également spécifier une adresse IP pour que les résultats renvoyés soient corrects.
- Si vos critères de filtrage renvoient un nombre excessif de composants retirés, l'interface REST ne renvoie aucune réponse. Utilisez d'autres options de filtrage pour réduire la quantité de résultats. D'autres critères de filtre sont disponibles à l'adresse http://*nom_hôte*:*port*/rest/retired/xsd/filterselect.xsd.

Suppressions de domaine IP

Vous pouvez supprimer des domaines IP. Par exemple, vous pouvez supprimer un domaine IP lors de la fusion de deux ou plusieurs domaines. Vous pouvez également supprimer un domaine IP qui a été utilisé à des fins d'analyse. La suppression d'un domaine IP supprime toutes les unités et les composants d'unité qui y sont associés. La suppression d'un domaine IP annule également le profil de détection associé à ce domaine IP.

Vous supprimez des domaines IP dans CA Performance Center. Après avoir supprimé un domaine IP, synchronisez la suppression avec Data Aggregator ou attendez la synchronisation automatique.

Remarque : Pour plus d'informations sur la suppression et la synchronisation des domaines IP, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

Une fois que Data Aggregator est informé qu'un domaine IP a été supprimé, les événements suivants se produisent :

- Toutes les unités et les composants d'unité qui sont associés au domaine IP supprimé sont supprimés.
- Le Data Collector associé au domaine IP supprimé est arrêté. L'état indique Aucune collecte de données.

  Remarque : Vous pouvez supprimer un domaine IP lorsque Data Collector est arrêté. Quand Data Collector est rétabli, un message d'erreur s'affiche dans le fichier *répertoire d'installation de Data Collector*/apache-karaf-2.3.0/shutdown.log et Data Collector s'arrête immédiatement.
- Tous les profils de détection qui spécifient le domaine IP supprimé sont annulés et ne peuvent pas être exécutés. L'état indique Aucun domaine IP. Toutes les détections en cours d'exécution dans un domaine IP supprimé sont abandonnées.

  Remarque : Vous pouvez modifier l'état d'un profil de détection annulé et le rétablir à l'état Prêt en spécifiant un domaine IP valide pour lequel vous souhaitez détecter des unités.
- Un événement d'audit est généré sur l'élément de client hébergé associé pour chaque unité supprimée.

Informations complémentaires :

Profils de détection (page 66)

Suppressions de client hébergé

Vous pouvez supprimer des clients hébergés. Par exemple, vous pouvez supprimer un client hébergé si vous êtes un fournisseur de services gérés (MSP) et si un client hébergé n'est plus votre client. La suppression d'un client hébergé supprime toutes les unités, les composants d'unité, les domaines IP, les profils SNMP et les profils de détection que vous avez associés à celui-ci.

Remarque : Vous ne pouvez pas supprimer le client hébergé par défaut.

Vous supprimez des clients hébergés dans CA Performance Center. Après avoir supprimé un client hébergé, synchronisez manuellement la suppression avec Data Aggregator ou attendez que la synchronisation automatique se produise.

Remarque : Pour plus d'informations sur la suppression et la synchronisation des clients hébergés, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

Une fois que Data Aggregator est informé qu'un client hébergé a été supprimé, les événements suivants se produisent :

- Toutes les unités, les composants d'unité, les domaines IP, les profils SNMP et les profils de détection qui sont associés au client hébergé supprimé sont supprimés.
- L'interrogation des unités supprimées et des composants d'unité est arrêtée.
- Les données historiques sur les unités supprimées et les composants des unités ne sont plus accessibles.
- Un événement d'audit est généré sur l'unité Data Aggregator pour chaque client hébergé supprimé.
- Tous les événements de seuil sur l'unité supprimée et ses composants supprimés sont supprimés.

Remarque : Vous pouvez supprimer un client hébergé lorsque Data Collector est arrêté. Un message d'erreur s'affiche dans le fichier *répertoire d'installation de Data Collector*/apache-karaf-2.3.0/shutdown.log lorsque Data Collector est réactivé, puis fermé immédiatement.

Désactivation des clients hébergés

Vous pouvez désactiver des clients hébergés. Par exemple, vous pouvez désactiver un client hébergé si vous êtes un fournisseur de services gérés (MSP) et que vous souhaitez arrêter la surveillance active de l'infrastructure de client hébergé.

Remarque : Pour pouvoir effectuer cette tâche, connectez-vous en tant qu'administrateur.

Vous désactivez des clients hébergés dans CA Performance Center. Après avoir désactivé un client hébergé, synchronisez la désactivation avec Data Aggregator ou attendez la synchronisation automatique.

Remarque : Pour en savoir plus sur la désactivation des clients hébergés, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

Une fois que le Data Aggregator est informé qu'un client hébergé a été désactivé, les opérations suivantes ont lieu :

- Le système Data Aggregator arrête tous les hôtes Data Collector qui sont associés au client hébergé désactivé. Les hôtes Data Collector indiquent alors un statut Aucune collecte de données. (Lorsque le client hébergé est réactivé, les hôtes Data Collector doivent être redémarrés manuellement.)

  Remarque : Pour toute nouvelle installation de Data Collector pour un client hébergé désactivé, le statut Aucune collecte de données est affiché. La détection est uniquement permise lorsque le client hébergé est activé à nouveau.
- Toutes les unités, les composants d'unité, les domaines IP, les profils SNMP et les profils de détection qui sont associés au client hébergé désactivé ne sont pas supprimés.
- L'interrogation s'arrête pour tous les composants et les unités qui sont surveillés pour le compte du client hébergé désactivé.
- Les données historiques sur les unités et les composants pour un client hébergé restent accessibles.
- Les profils de détection associés au client hébergé désactivé sont annulés et ne peuvent pas être exécutés. Les profils de détection indiquent l'état Client hébergé désactivé.
- Si un profil de détection est annulé pendant qu'une détection est en cours, la détection est interrompue.
- Un événement d'audit est généré sur l'unité Data Aggregator pour le client hébergé désactivé.

Informations complémentaires :

Activation des clients hébergés (page 109)

Activation des clients hébergés

Vous pouvez activer un client hébergé que vous avez désactivé préalablement. Par exemple, vous pouvez activer un client hébergé si vous êtes un fournisseur de services gérés (MSP) et que vous souhaitez redémarrer la surveillance active de l'infrastructure de client hébergé.

Remarque : Pour pouvoir effectuer cette tâche, connectez-vous en tant qu'administrateur.

Vous activez des clients hébergés dans CA Performance Center. Après avoir activé un client hébergé, effectuez les actions suivantes :

1. Synchronisez l'activation avec Data Aggregator ou attendez la synchronisation automatique.

   Remarque : Pour en savoir plus sur l'activation des clients hébergés, reportez-vous au *Manuel de l'administrateur* de CA Performance Center.

   Les résultats suivants se produisent :

   - Data Aggregator est informé qu'un client hébergé a été activé.
   - Les profils de détection qui sont associés au client hébergé activé sont validés. Les profils de détection affichent leur état actuel.
   - Un événement d'audit est généré sur l'unité Data Aggregator pour le client hébergé.

2. Redémarrez manuellement tous les hôtes Data Collector qui sont associés au client hébergé (page 53).

   Les résultats suivants se produisent :

   - L'interrogation redémarre pour tous les composants et les unités qui sont surveillés pour le compte du client hébergé activé.
   - Les profils de détection associés au client hébergé activé peuvent être exécutés.

Informations complémentaires :

Désactivation des clients hébergés (page 107)
Dépannage : la détection ne démarre pas (page 169)

Reconfiguration des unités

Vous pouvez surveiller les modifications apportées à la reconfiguration des unités automatiquement ou manuellement dans Data Aggregator pour maintenir les composants d'unité actualisés. La reconfiguration des unités inclut la modification des composants des unités physiques et de la configuration logicielle, sous forme de tests du chemin de réponse de surveillance des protocoles par exemple. Data Aggregator utilise la même méthode pour surveiller les deux types de reconfiguration.

Exemples supplémentaires de modifications de la reconfiguration :

- L'ajout d'une carte à une unité, qui ajoute des ports supplémentaires à l'unité.
- L'ajout de mémoire, d'unités centrales, d'interfaces physiques ou d'une famille de mesures à une unité détectée.
- Reconfiguration d'un commutateur virtuel.
- Changement de la configuration d'une unité de manière à ce qu'une unité détectée participe à des protocoles de routage.

Lorsqu'une modification est détectée, Data Aggregator génère des événements de reconfiguration et peut mettre à jour sa représentation de la famille de mesures afin de refléter les modifications apportées aux composants d'unité. Affichez les événements de reconfiguration en sélectionnant Tableaux de Bord, Opérations, Affichage d'événements.

La compréhension du fonctionnement de la détection des changements dans Data Aggregator vous aide à sélectionner les options les mieux appropriées pour la reconfiguration d'unité de surveillance dans votre environnement. Par exemple, vous pouvez définir la fréquence de la surveillance de détection des modifications.

Informations complémentaires :

Gestion de la détection des modifications (page 110)

Gestion de la détection des modifications

La planification de la gestion de la détection des modifications permet de garantir que Data Aggregator détecte et surveille les reconfigurations des unités de votre environnement selon vos besoins. Vous pouvez planifier la reconfiguration d'unités lors de la première configuration de Data Aggregator pour la détection des nouvelles unités ou modifier ces options à tout moment une fois les unités détectées.

Les choix que vous faites dépendent :

- De la probabilité de la modification
- De la fréquence de la modification prévue
- Du nombre de données obsolètes autorisées

Il peut y avoir des familles de mesures, comme les unités centrales, pour lesquelles vous voulez surveiller la reconfiguration de façon ponctuelle. Pour d'autres familles de mesures plus dynamiques, comme les systèmes virtuels, choisissez un taux plus fréquent.

Processus de base de définition de la détection des modifications :

1. Créez ou modifiez un profil de surveillance *personnalisé*. (Vous pouvez également copier un profil de surveillance prédéfini et modifier la copie.)
2. Sélectionnez Activer la détection des modifications et définissez les paramètres de détection des modifications ainsi que le taux dans le profil de surveillance.

   L'option Taux (sous Paramètres de détection des modifications) est utilisée pour définir la fréquence à laquelle Data Aggregator recherche les modifications. Vous pouvez définir le taux d'interrogation en minutes ou en heures. Par défaut, le taux est défini sur 24 heures.

   Remarque : Prenez en compte la fréquence de modification possible de la famille de mesures ainsi que le nombre d'unités auxquelles le profil de surveillance est appliqué. Evitez les fréquences de détection des modifications des paramètres d'une valeur plus élevée que nécessaire.

3. Mettez à jour la représentation des familles de mesures générée par Data Aggregator.

   Une fois que vous avez défini le taux de détection des modifications, vous pouvez utiliser l'une des deux méthodes de correction de la configuration de Data Aggregator : mise à jour automatique ou mise à jour manuelle des familles de mesures. Cette option ne procède pas à la mise à jour des familles de mesures, mais elle met à jour leur représentation en vérifiant que l'ensemble de composants surveillé est correct.

   - La sélection de l'option Mise à jour automatique des familles de mesures (sélectionnée par défaut) signifie que vous ne devez pas intervenir lorsqu'une reconfiguration est détectée. Data Aggregator lance la surveillance automatique des nouveaux composants et retire tout composant qui n'est plus détecté lorsqu'un événement de reconfiguration se produit.

     Affichez le tableau de bord Affichage des événements pour consulter les événements de reconfiguration :

     - Si les composants ont été modifiés pour une unité, un événement est généré sur l'unité associée. Cet événement indique qu'une modification de composant a été détectée et qu'elle sera appliquée après un court délai.
     - Suite au rapprochement de composant, un autre événement est généré. Cet événement indique le nombre de composants ajoutés, retirés et non modifiés

   - Si vous désélectionnez l'option Mise à jour automatique des familles de mesures, Data Aggregator ne démarrera pas automatiquement la surveillance des nouveaux composants ou ne retirera pas les anciens composants.

     Affichez le tableau de bord Affichage des événements pour consulter les événements de reconfiguration :

     - Si les composants ont été modifiés pour une unité, un événement est généré sur l'unité associée. Cet événement indique qu'une modification de composant s'est produite, mais que le rapprochement ne s'est pas produit.

     Pour appliquer les modifications de reconfiguration, cliquez manuellement sur le bouton Mettre à jour la famille de mesures dans la page Familles de mesures interrogées pour une unité.

4. Pour activer le profil de surveillance personnalisé, affectez-le à une collection d'unités.

Exemples :

- Si vous pensez que votre environnement subira des opérations de maintenance importantes, vous pouvez désactiver la mise à jour automatique et attendre la fin de ces opérations. Pour des modifications standard moins importantes, l'activation de la fonctionnalité de mise à jour automatique permet de garantir la mise à jour constante de Data Aggregator.
- Les profils de surveillance sont affectés à des collections qui contiennent des unités. Si vous souhaitez utiliser une méthode différente de surveillance des unités spécifiques, créez une collection d'unités personnalisée pour ces unités et affectez un profil de surveillance personnalisé avec les paramètres de détection des modifications de votre choix. Par exemple, vous pouvez surveiller des routeurs principaux critiques plus fréquemment que d'autres routeurs en créant une collection de routeurs principaux critiques et en affectant un profil de surveillance personnalisé destiné à détecter les modifications toutes les heures. Les autres routeurs peuvent rester dans la collection d'unités All Routers (Tous les routeurs) et utiliser le profil de surveillance prédéterminé (sans détection des modifications) ou un profil de surveillance personnalisé pour lequel la détection des modifications est moins fréquente.

Informations complémentaires :

Détection et interrogation (page 63)
Mise à jour manuelle de la reconfiguration des unités (page 114)
Mise à jour automatique de la reconfiguration des unités (page 113)

Mise à jour automatique de la reconfiguration des unités

Les modifications de la reconfiguration d'une unité détectée peuvent affecter les familles de mesures qui sont associées à l'unité. Vous pouvez définir la reconfiguration des unités pour qu'elle se mette à jour automatiquement dans le profil de surveillance auquel les familles de mesures sont affectées et qui s'applique à toutes les familles de mesures que le profil de surveillance inclut. Cette option est définie par défaut quand vous créez un profil de surveillance personnalisé, mais vous pouvez également la modifier à tout moment. Cette procédure indique le mode de définition de l'option Mise à jour automatique des familles de mesures dans un profil de surveillance personnalisé existant si elle a préalablement été désélectionnée.

Lorsque la famille de mesures est mise à jour, Data Aggregator dispose d'une représentation précise de la configuration d'unité. Les rapports que vous générez reflètent des informations exactes.

Procédez comme suit :

1. Accédez à la liste de tous les profils de surveillance.

2. Sélectionnez le profil de surveillance que vous voulez mettre à jour automatiquement et cliquez sur Modifier.
3. Sélectionnez Activer la détection des modifications , puis procédez comme suit :
   - Sélectionnez les paramètres de détection des modifications et définissez le taux sur une valeur supérieure à zéro.

     Remarque : Prenez en compte la fréquence de modification possible de la famille de mesures ainsi que le nombre d'unités auxquelles le profil de surveillance est appliqué. Evitez les fréquences de détection des modifications des paramètres d'une valeur plus élevée que nécessaire.
   - Sélectionnez Mise à jour automatique des familles de mesures.
   - Cliquez sur Enregistrer.

   Lorsque vous effectuez un changement de configuration pour une unité associée à ce profil de surveillance, la configuration d'unité est mise à jour automatiquement.

   Lorsqu'une configuration d'unité est mise à jour, Data Aggregator réalise les étapes suivantes :

   - Génération d'un événement sur l'unité surveillée.
   - Identification et création des nouveaux composants.
   - Identification et suppression des composants qui ne sont plus présents

     Remarque : Par défaut, les composants retirés ne sont pas synchronisés avec CA Performance Center. Pour activer cette option, cochez la case Synchroniser les éléments retirés dans la boîte de dialogue Modifier la source des données de la page Gérer les sources de données de CA Performance Center.
   - Identification des composants existants modifiés par rapport à une détection précédente Le contenu de la colonne Nom change, le cas échéant.

     Remarque : Les données historiques sont accessibles et peuvent être rapportées.

Informations complémentaires :

Gestion de la détection des modifications (page 110)

Mise à jour manuelle de la reconfiguration des unités

Les modifications de la reconfiguration d'une unité détectée peuvent affecter les familles de mesures qui sont associées à l'unité. Vous pouvez mettre à jour la reconfiguration des unités manuellement lorsque l'option Mise à jour automatique des familles de mesures n'est pas sélectionnée dans le profil de surveillance associé. Dans ce cas, vous affichez les journaux d'événements pour identifier les événements de reconfiguration pour lesquels vous voulez mettre à jour les familles de mesures.

Lorsque la famille de mesures est mise à jour, Data Aggregator dispose d'une représentation précise de la configuration d'unité. Les rapports que vous générez reflètent des informations exactes.

Procédez comme suit :

1. Affichez les journaux d'événements pour identifier les événements de reconfiguration pour lesquels vous souhaitez mettre à jour les familles de mesures (page 149).
2. Cliquez sur Unités surveillées dans le menu Inventaire surveillé d'une source de données de Data Aggregator.

   L'onglet Arborescence s'ouvre.
3. A partir de la liste déroulante, sélectionnez Unité par collection, puis sélectionnez l'unité surveillée que vous avez mise à jour parmi l'arborescence correspondante.

   L'onglet Familles de mesures interrogées indique les profils de surveillance consolidés associés à une unité. Les unités ont un seul profil de surveillance consolidé. Chaque profil de surveillance consolidé répertorie toutes les familles de mesures qui peuvent être interrogées sur l'unité et indique si l'unité prend en charge la famille de mesures.
4. Sélectionnez la famille de mesures pour laquelle vous voulez mettre à jour la configuration et cliquez sur Mettre à jour la famille de mesures.

   Votre configuration d'unité est mise à jour et Data Aggregator effectue les étapes suivantes :

   - Génération d'un événement sur l'unité surveillée.
   - Identification et création des nouveaux composants.
   - Identification et suppression des composants qui ne sont plus présents

     Remarque : Par défaut, les composants retirés ne sont pas synchronisés avec CA Performance Center. Pour activer cette option, cochez la case Synchroniser les éléments retirés dans la boîte de dialogue Modifier la source des données de la page Gérer les sources de données de CA Performance Center.
   - Identification des composants existants modifiés par rapport à une détection précédente Le contenu de la colonne Nom change, le cas échéant.

     Remarque : Les données historiques sont accessibles et peuvent être rapportées.

Informations complémentaires :

Affichage des unités surveillées (page 99)
Gestion de la détection des modifications (page 110)

Chapitre 5: Gestion des interfaces

Ce chapitre traite des sujets suivants :

Interrogation des interfaces critiques plus rapide que celles des interfaces non critiques (page 117)
Méthode de définition et d'activation d'un filtre d'interface (page 129)
Suppression d'un filtre d'interface (page 131)
Convention d'attribution de nom de composants d'interface (page 132)
Calcul de l'utilisation de l'interface (page 132)

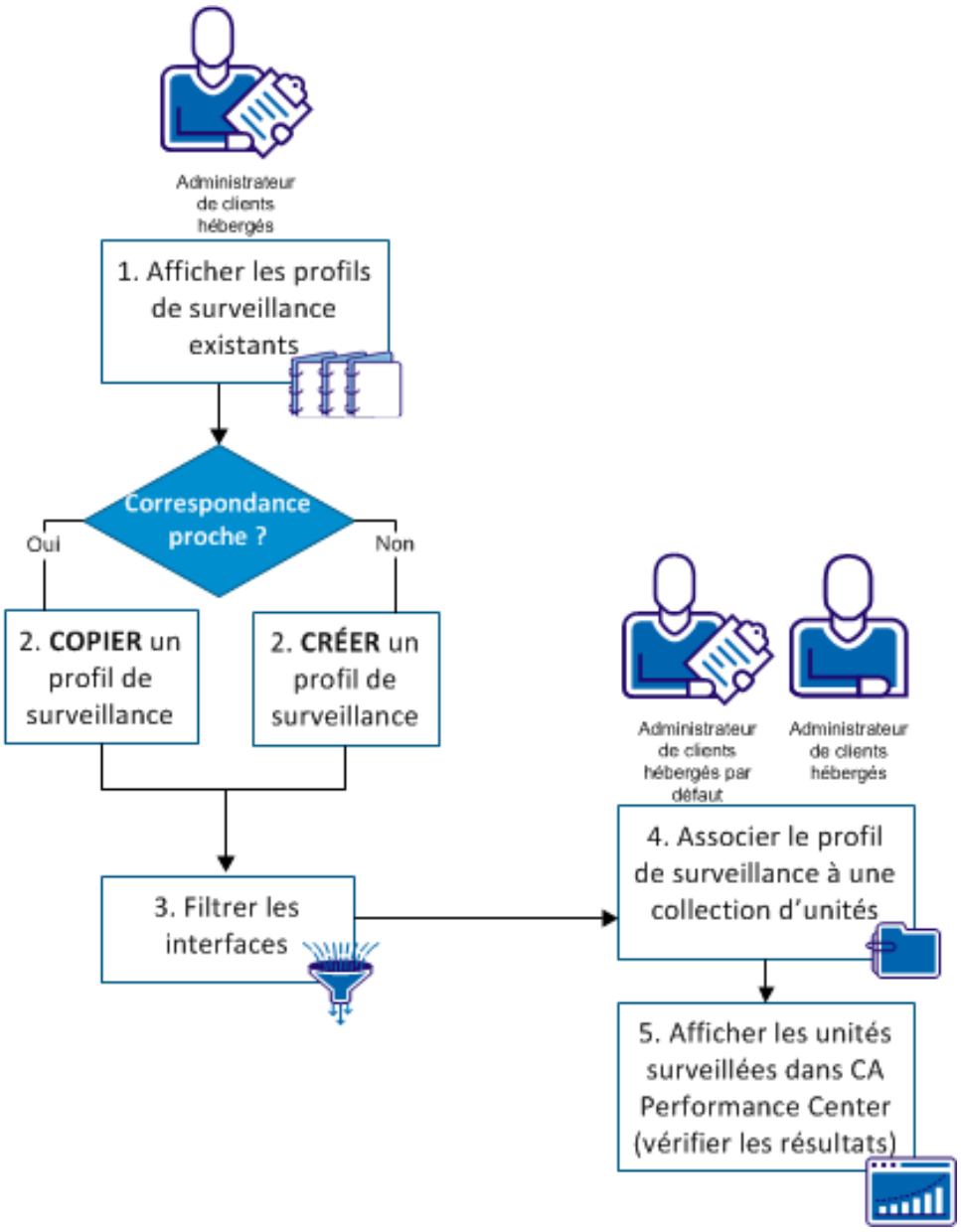
Interrogation des interfaces critiques plus rapide que celles des interfaces non critiques

En tant qu'administrateur, vous devez disposer de données récentes concernant les systèmes les plus importants lorsque vous augmentez les performances globales des systèmes de gestion d'infrastructures. Pour cela, vous pouvez interroger uniquement les interfaces critiques à une fréquence élevée et en interrogeant les interfaces non critiques à une fréquence normale ou faible. L'interrogation de la famille de mesures d'interface à des fréquences différentes associée à votre profil de surveillance est possible grâce à un filtre. L'interrogation à une vitesse élevée des interfaces de façon sporadique permet de réduire le trafic réseau inutile et la charge du système de gestion d'infrastructures tout en continuant à surveiller l'intégrité de votre système de réseau.

Envisageons, par exemple, que votre commutateur d'accès au centre de données relie un grand nombre de serveur d'applications à seulement deux commutateurs d'agrégation. Vous décidez d'interroger les interfaces prenant en charge ces commutateurs d'agrégation à une fréquence plus élevée. Ces liens sont primordiaux, étant donné qu'ils prennent en charge le trafic réseau vers tous les autres commutateurs connectés. Toutefois, l'interrogation de *toutes* les interfaces à une fréquence supérieure risque d'entraîner un trafic réseau inutile, le gaspillage des ressources système et, sans doute, des problèmes de performance du réseau. Après avoir consulté les équipes opérations réseau et ingénierie de votre entreprise, vous décidez qu'une fréquence d'interrogation standard suffit pour les interfaces de connexion à chaque serveur relié. Pour appliquer des fréquences d'interrogation différentes, implémentez deux profils de surveillance pour les interfaces.

Remarque : Les filtres que vous définissez au niveau de la famille de mesures Interfaces sont ignorés lorsque les règles d'événement appliquées aux profils de surveillance déclenchent des événements.

L'illustration suivante indique la procédure à suivre pour configurer les profils de surveillance dans le cadre de l'interrogation des interfaces à des fréquences variables :



Procédures
Affichage des profils de surveillance existants (page 119)
Copie du profil de surveillance prédéfini Interface de réseau (page 120)
Définition d'un filtre au niveau de la famille de mesures d'interface (page 122)

Procédures
Association du profil de surveillance à une collection d'unités (page 125)
Affichage des unités surveillées pour vérifier les résultats (page 126)

Remarque : Pour plus d'informations sur le fonctionnement des profils de surveillance avec les collections d'unités et les familles de mesures, reportez-vous au *Manuel de présentation de Data Aggregator*.

Affichage des profils de surveillance

En tant qu'administrateur de CA Performance Center, vous décidez d'interroger des interfaces critiques aussi souvent que possible. Toutefois, vous souhaitez également réduire le trafic réseau inutile que l'interrogation de *toutes* les interfaces à une fréquence élevée peut entraîner. Vous décidez de créer deux profils de surveillance pour les interfaces, l'un à une fréquence d'interrogation normale, l'autre à une fréquence d'interrogation élevée.

Avant de créer un profil de surveillance, vous révisez les profils de surveillance existants afin de vérifier si l'un d'entre eux répond à vos besoins.

Procédez comme suit :

1. Dans le menu Configuration de la surveillance, cliquez sur "Profils de surveillance" pour une source de données de Data Aggregator.

   Une liste de profils de surveillance est remplie.

2. Sélectionnez un profil de surveillance.

   Les détails du profil de surveillance sélectionné sont insérés dans les onglets, comme suit :

   - L'onglet Familles de mesures affiche une liste des familles de mesures associées à ce profil de surveillance. Les familles de mesures contiennent les mesures qui sont utilisées pour interroger les unités et les composants.
   - L'onglet Collections affiche une liste des collections d'unités associées à ce profil de surveillance.

Informations complémentaires :

Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)

Copie d'un profil de surveillance prédéfini

En tant qu'administrateur de CA Performance Center, vous décidez que le profil de surveillances prédéfini Interfaces réseau satisfait entièrement vos besoins et requiert des modifications mineures. Par conséquent, vous créez une copie et l'utilisez pour interroger uniquement les interfaces critiques à une fréquence d'interrogation plus élevée.

Remarque : Pour pouvoir effectuer cette tâche, connectez-vous en tant qu'administrateur.

Procédez comme suit :

1. Accédez à la liste de tous les profils de surveillance dans CA Performance Center (page 119).
2. Sélectionnez le profil de surveillance Interfaces réseau et cliquez sur Copier.

   Remarque : Vous ne pouvez pas modifier ni supprimer les profils de surveillance prédéfinis. Tous les profils de surveillance, y compris les profils personnalisés, sont globaux.

   La boîte de dialogue Créer/modifier un profil de surveillance s'ouvre.
3. Entrez les informations suivantes pour votre profil de surveillance :
   - **Nom :** Interfaces de liaison montante
   - **Description** (facultative**) :** surveille les performances des interfaces des principales unités de liaison montante.
   - **Fréquence d'interrogation SNMP :** 1 minute

   Remarque : Nous vous recommandons de renommer le profil. L'attribution d'un nom unique est appliquée à tous les clients hébergés.

   Tenez compte des informations suivantes concernant les fréquences d'interrogation :

   - Lorsque la fréquence d'interrogation est modifiée, il faut jusqu'à deux cycles pour que la nouvelle fréquence d'interrogation prenne effet. Lorsque la fréquence de 60 minutes est utilisée pour interroger une unité existante, le message "Aucune donnée n'est disponible" apparaît dans la vue du tableau de bord avec la plage horaire par défaut Dernière heure. Pour visualiser des données plus anciennes, définissez la valeur du tableau de bord sur une heure antérieure. Toutefois, la vue n'affiche pas les toutes dernières données tant que le nouveau cycle d'interrogation n'est pas terminé.
   - Les interfaces qui sont affectées à plusieurs profils de surveillance avec différentes fréquences d'interrogation sont interrogées selon la fréquence affectés la plus courte.

4. Dans les paramètres de détection des modifications, laissez la valeur de taux sur 24 heures.

   Tenez compte des informations suivantes concernant les fréquences de détection des modifications :

   - La *fréquence de détection des modifications* est la fréquence à laquelle Data Aggregator vérifie si les composants sur une unité ont été reconfigurés. Les modifications peuvent inclure la création de composants ou le retrait de composants existants.

     Remarque : L'algorithme de rapprochement spécifié dans la famille de mesures définit les modifications de configuration à surveiller. Pour plus d'informations sur la détection des changements et la procédure de reconfiguration d'unités, consultez le *Manuel de l'administrateur de Data Aggregator*.

   - L'option Taux (sous Paramètres de détection des modifications) est utilisée pour définir la fréquence à laquelle Data Aggregator recherche les modifications. Vous pouvez définir le taux d'interrogation en minutes ou en heures. Par défaut, le taux est défini sur 24 heures.

   - Les modifications sont détectées à la fréquence la plus élevée spécifié pour tous les profils de surveillance associés à une collection d'unités.

5. N'activez pas la case à cocher Mettre automatiquement à jour les familles de mesures.

   Cette option contrôle la réponse de Data Aggregator une fois qu'une modification ou qu'une reconfiguration est détectée. La sélection de cette option entraîne automatiquement le lancement de la surveillance des nouveaux composants ou l'arrêt de la surveillance des composants retirés, par Data Aggregator. Lorsque cette option n'est pas sélectionnée, vous pouvez contrôler manuellement la surveillance des composants, en procédant comme suit :

   a. Activez le tableau de bord Affichage des événements pour surveiller les événements de configuration.

   b. Dans le menu Administration de Data Aggregator, sélectionnez Unités surveillées, puis la vue Familles de mesures interrogées.

   c. Sélectionnez la famille de mesures appropriée et cliquez sur Mettre à jour la famille de mesures pour garantir la récupération de dernière reconfiguration de cette unité par Data Aggregator.

   Remarque : Si un filtre d'interface est appliqué, Data Aggregator surveille uniquement les interfaces qui transfèrent les conditions de filtre après la reconfiguration.

6. Conservez la famille de mesures Interfaces comme seule famille de mesures dans la liste Familles de mesures sélectionnées.
7. Cliquez sur Enregistrer.

   Le profil de surveillance que vous avez copié est ajouté à la liste Profils de surveillance. Toutefois, ce profil de surveillance ne deviendra actif que lorsque vous l'aurez affecté à une collection d'unités.

Informations complémentaires :

Détection et interrogation (page 63)
Affichage des événements (page 149)
Gestion de la détection des modifications (page 110)
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Flux de travaux de détection (page 60)
Méthode de définition et d'activation d'un filtre d'interface (page 129)

Définition d'un filtre d'interface

Par défaut, le profil de surveillance Interface réseau prédéfini inclut un filtre pour empêcher la modélisation des interfaces qui sont désactivées pour l'administration. Le filtrage réduit le nombre d'interfaces surveillées, réduisant ainsi la collection des données superflues et le trafic réseau.

En plus d'interroger uniquement les interfaces d'administration activées, vous pouvez également interroger les interfaces critiques plus fréquemment. Pour isoler et interroger uniquement les interfaces les plus rapides, ajoutez une deuxième condition de filtre au filtre d'interface associé à votre profil de surveillance personnalisé. Cette deuxième condition de filtre isole les interfaces critiques en recherchant uniquement les interfaces qui contiennent le terme "liaison montante" (uplink) dans leur description.

Remarque : Pour pouvoir effectuer cette tâche, connectez-vous en tant qu'administrateur.

Procédez comme suit :

1. Sélectionnez votre profil de surveillance d'interfaces (appelé "Interfaces de liaison montante") dans la page Profils de surveillance (page 120).
2. Cliquez sur la ligne de la famille de mesures Interface dans l'onglet Familles de mesures et cliquez sur Modifier le filtre.

   Remarque : Ne cliquez pas directement sur le nom de la famille de mesures, car il est lié de manière à vous mener directement à la définition de la famille de mesures. Cliquez plutôt sur la ligne contenant le nom de la famille de mesures pour activer l'option Modifier le filtre.

3. Cliquez sur le bouton Ajouter une condition.

   Remarque : Plusieurs conditions sont associées à une opération "et", ce qui signifie que toutes les conditions doivent être remplies pour que le filtre soit satisfait.

4. Configurez les conditions de filtre avec les options suivantes et cliquez sur Enregistrer :

   - Attribut : Description
   - Opération : Contient
   - Valeur de filtre : Liaison montante

   Remarque : Le champ Valeur de filtre est sensible à la casse.

   Prenez en compte les informations suivantes concernant les attributs supplémentaires que vous pouvez utiliser pour le filtrage :

   - Pour les options Vitesse en entrée et Vitesse en sortie, vous pouvez entrer une valeur décimale en Kbit/s, Mbit/s ou Gbit/s dans le champ de texte (1,544 par exemple).
   - Pour plus d'informations sur la configuration du type (ifType), accédez au site Web d'iana : http://www.iana.org/assignments/ianaiftype-mib http://www.iana.org/assignments/ianaiftype-mib.
   - Pour les options Description et Alias, vous pouvez utiliser une expression régulière pour activer le filtrage uniquement lorsque vous sélectionnez l'opération Correspond à une expression régulière ou Ne correspond pas à une expression régulière.

   Lorsque vous enregistrez les modifications, les critères de filtre s'affichent dans l'onglet Familles de mesures. Vous pouvez à présent appliquer ce profil de surveillance à la collection appropriée pour lancer l'interrogation des interfaces que vous avez sélectionnées.

Remarque : Data Aggregator procède au filtrage une fois la détection terminée. Les éléments d'interface qui ne correspondent pas aux critères de filtrage ne sont pas interrogés. Si vous ajoutez ou modifiez un filtre d'interface *après* avoir exécuté une détection, l'interrogation de ces éléments s'arrête. Ces éléments d'interface ne sont pas *affichés* dans les tableaux de bord et les vues de données CA Performance Center.

Remarques concernant les filtres d'interface et les profils de surveillance multiples

Lorsque plusieurs profils de surveillance sont affectés à une collection d'unités, les critères de filtre respectent la règle "ou". Data Aggregator surveille donc toutes les interfaces qui répondent aux critères pour l'un des profils de surveillance appartenant au groupe.

Il est possible d'attribuer des filtres à certains profils de surveillance uniquement. De plus, ces profils peuvent spécifier des fréquences d'interrogation différents. Dans ce cas, Data Aggregator surveille les interfaces qui correspondent à un profil de surveillance, mais dont les fréquences d'interrogation peuvent être différentes. Si plusieurs profils de surveillance sont appliqués à une interface, Data Aggregator interroge l'interface à une seule reprise et à la fréquence d'interrogation la plus élevée.

- Filtre du profil de surveillance 1 : la description contient un "X" et la fréquence d'interrogation est de 1 minute.
- Filtre du profil de surveillance 2 : aucun ; fréquence d'interrogation de 5 minutes
- Filtre du profil de surveillance 3 : la description contient un "Y" et la fréquence d'interrogation est de 10 minutes.

Dans cet exemple, les interfaces qui correspondent au profil de surveillance 1 sont interrogées toutes les minutes, alors que toutes les autres interfaces sont interrogées toutes les 5 minutes. Les interfaces qui correspondent au profil de surveillance 3 correspondent également au profil de surveillance 2, qui n'inclut pas de filtre. La fréquence d'interrogation la plus élevée est appliquée et aucune interface n'est donc interrogée à un intervalle de 10 minutes.

Dans ce cas, si aucun filtre n'est défini pour un profil de surveillance, un grand nombre d'interfaces peuvent être interrogées plus fréquemment que nécessaire. Cela signifie qu'après avoir défini un filtre, vous devez supprimer les associations au niveau des autres profils de surveillance pour être sûr que seuls les composants correspondant au filtre spécifié sont surveillés.

Affectation d'un profil de surveillance à une collection d'unités

En tant qu'administrateur ou administrateur de clients hébergés, vous êtes chargé d'associer le nouveau profil de surveillance Interfaces de liaison montante à une collection d'unités pour lancer l'interrogation. Pour cela, vous associez le profil à la collection de commutateurs, c'est-à-dire à la collection d'unités associée au profil de surveillance prédéfini Interfaces réseau. Les fréquences d'interrogation sont appliquées aux interfaces de cette collection d'unités, comme suit :

- Interrogation rapide : interfaces qui satisfont les critères de filtrage du profil de surveillance Interfaces de liaison montante.
- Interrogation normale : toutes les autres interfaces détectées par le profil de surveillance Interfaces réseau.

Important : Tous les profils de surveillance personnalisés sont globaux et visibles pour les administrateurs de clients hébergés. Toutefois, vous pouvez limiter à un client hébergé l'association d'un profil de surveillance avec une collection d'unités spécifique.

Procédez comme suit :

1. Dans le menu Configuration de la surveillance correspondant à la source de données Data Aggregator, cliquez sur Collections.

   Une liste de collections d'unités s'affiche. Les administrateurs peuvent afficher les collections d'unités associées au client hébergé qu'ils administrent. Un administrateur de clients hébergés peut afficher sa propre liste (client hébergé) de collections d'unités.

2. Sélectionnez la collection d'unités All Switches (Tous les commutateurs) et cliquez sur l'onglet Profils de surveillance.

   Une liste affiche les profils de surveillance qui sont associés à la collection d'unités sélectionnée. La collection d'unités Interface réseau figure déjà dans cette liste.

3. Cliquez sur Gérer.

   La boîte de dialogue Assigner des profils de surveillance de collection s'ouvre.

4. Sélectionnez le profil de surveillance Interfaces de liaison montante et cliquez sur Ajouter.

   Le profil de surveillance sélectionné est ajouté à la liste Profils de surveillance affectés.

5. Cliquez sur Enregistrer.

   Vos modifications sont enregistrées.

Informations complémentaires :

Associations de profils de surveillance prédéfinis (page 89)
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Flux de travaux de détection (page 60)
Méthode de définition et d'activation d'un filtre d'interface (page 129)

Affichage des unités surveillées pour vérifier les résultats

Après avoir configuré vos profils de surveillance, révisez les unités surveillées et le rapport de filtrage pour vérifier que seules vos unités critiques sont interrogées à la fréquence la plus élevée. Ces informations vous aident à voir des informations en contexte, par exemple pour identifier les profils de surveillance utilisés pour interroger des composants d'unité. La vérification des résultats peut vous aider à identifier les réglages nécessaires pour vous permettre d'atteindre les objectifs que vous vous êtes fixés en matière d'interrogation.

Remarque : Les unités surveillées sont des unités gérables ou qui acceptent la commande ping (accessibles mais non gérables). Les unités inaccessibles ne sont pas des unités surveillées. Vous pouvez afficher les composants des unités surveillées à partir de l'onglet Familles de mesures interrogées.

Procédez comme suit :

1. Exécutez une détection à la demande.

   Remarque : Si votre profil de détection s'exécute automatiquement, vous pouvez patienter jusqu'à la détection planifiée suivante. Pour plus d'informations sur la gestion de la détection, reportez-vous au *Manuel de l'administrateur de Data Aggregator*.

2. Cliquez sur Unités surveillées dans le menu Inventaire surveillé d'une source de données de Data Aggregator.

3. Sélectionnez une de ces options dans la liste déroulante pour localiser une de vos unités de commutateur d'agrégation dans l'arborescence correspondante :

   - Unité par collection : vos unités s'affichent dans la collection d'unités All Switches (Tous les commutateurs).
   - Unité par profil de surveillance : vos interfaces critiques apparaissent dans Unités sous le profil de surveillance Uplink Interfaces (Interfaces de liaison montante).

   Remarque : Vous pouvez aussi sélectionner l'onglet Recherche pour effectuer une recherche par nom d'hôte, nom d'unité ou adresse IP. Vous pouvez entrer un nom ou une adresse IP partielle pour renvoyer une liste d'unités qui contiennent cette correspondance partielle. Les caractères génériques et les expressions régulières ne sont pas pris en charge.

L'onglet Familles de mesures interrogées indique les profils de surveillance consolidés associés au commutateur. Les unités possèdent un seul profil de surveillance consolidé. Chaque profil de surveillance consolidé répertorie toutes les familles de mesures à interroger sur l'unité et indique si l'unité prend en charge la famille de mesures.

4. Sélectionnez la famille de mesures d'interface.

   Le tableau de composants de la famille de mesures d'interface indique l'un des statuts d'interrogation suivants pour les composants d'interface détectés :

   Actif

   Indique que le composant est en cours d'interrogation.

   Inactive

   Indique que l'interrogation sur le composant est arrêtée, car la famille de mesures n'est plus surveillée pour l'unité.

   Retiré

   Indique que le composant n'existe plus sur l'unité physique. L'interrogation sur le composant est arrêtée. Vous pouvez afficher des données historiques à des fins de génération de rapports. Par défaut, les composants retirés ne sont pas synchronisés avec CA Performance Center. Pour activer cette option, cochez la case Synchroniser les éléments retirés dans la boîte de dialogue Modifier la source des données de la page Gérer les sources de données de CA Performance Center.

   Filtré (composants d'interface uniquement)

   Indique que le composant ne transfère pas les critères de filtre et que l'interrogation sur le composant est arrêtée.

   Remarque : Les interfaces filtrées ne sont pas affichées dans les tableaux de bord et les vues de données CA Performance Center.

5. (Facultatif) Sélectionnez la famille de mesures d'interface et cliquez sur Mettre à jour la famille de mesures.

   Data Aggregator reconfigure les composants pour toutes les mises à jour de configuration. Par exemple, si vous ajoutez un lecteur de disque sur un serveur, vous pouvez utiliser le bouton Mettre à jour la famille de mesures pour redétecter la mise à jour de configuration. La mise à jour de configuration crée un composant de disque.

6. Cliquez sur l'onglet Rapport de filtre et procédez comme suit :

   a. Comparez les filtres sur chacun des autres profils de surveillance d'interface pour vérifier s'ils surveillent la même collection d'unités que celle que vous souhaitez filtrer.

   b. Supprimez toute relation entre les autres profils de surveillance d'interface et les collections d'unités qui bloqueront vos critères de filtre (page 92). Par exemple, si votre nouveau profil de surveillance d'interface est associé à la collection d'unités All Routers (Tous les routeurs), supprimez la relation entre les *autres* profils de surveillance d'interface et la collection d'unités All Routers (Tous les routeurs).

   c. Exécutez une autre détection et examinez le rapport de filtre mis à jour pour vérifier que les nouveaux critères de filtre sont actifs. Si le rapport de filtre indique qu'un profil de surveillance superflu a été inclus, répétez les étapes précédentes pour surveiller uniquement les interfaces souhaitées.

   L'onglet Filtrer le rapport indique les critères de filtre de l'interface qui ont été utilisés pendant la détection de composant. L'onglet présente également un rapport de toutes les interfaces identifiées sur l'unité et indique si elles correspondent aux critères de filtre spécifiés.

   Remarque : Si vous modifiez les règles d'un profil de surveillance personnalisé, le volet Critères de filtrage de l'interface ne reflète pas ces modifications. Si vous dissociez le profil de surveillance d'un groupe, le volet Critères de filtrage de l'interface ne reflète pas ces modifications. Redétectez l'unité pour filtrer les interfaces qui sont basées sur les modifications que vous avez apportées aux critères de filtrage et au profil de surveillance.

Informations complémentaires :

Détection et interrogation (page 63)
Mise à jour manuelle de la reconfiguration des unités (page 114)
Suppression d'un filtre d'interface (page 131)
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Méthode de définition et d'activation d'un filtre d'interface (page 129)

Méthode de définition et d'activation d'un filtre d'interface

Par défaut, le profil de surveillance d'interface réseau inclut un filtre pour empêcher la modélisation des interfaces désactivées pour l'administration. De plus, les interfaces avec un type (ifType) de valeur 1 (Autre) ou 24 (Bouclage) ne sont pas modélisées, qu'elles soient désactivées pour l'administration ou non. Les accords de niveau de service IP dont l'objet MIB rttMonCtrlAdminOwner contient la chaîne "Intégrité du réseau" ne sont pas modélisés non plus.

Le filtrage réduit le nombre d'interfaces surveillées, réduisant ainsi la collection de données superflue. Pour votre profil de surveillance *personnalisé*, vous pouvez spécifier des filtres supplémentaires pour les interfaces.

Remarque : Les filtres que vous définissez au niveau de la famille de mesures Interfaces sont ignorés lorsque les règles d'événement appliquées aux profils de surveillance déclenchent des événements.

Les critères de correspondance de filtre suivent la règle "OR" lorsque plusieurs profils de surveillance d'interface sont affectés à une collection d'unités. Dans ce cas, l'interface correspondant à n'importe lequel des critères de filtre est surveillée.

Vous pouvez ajouter ou modifier un filtre d'interface avant ou après l'exécution d'une détection. Data Aggregator procède au filtrage une fois la détection terminée. Seules les interfaces correspondant aux critères de filtre sont interrogées. Si vous ajoutez ou modifiez un filtre d'interface *après* avoir exécuté une détection, l'interrogation de ces interfaces s'arrête. Ces interfaces n'apparaissent *pas* dans les tableaux de bord et les vues de données CA Performance Center.

Remarque : Pour pouvoir effectuer cette tâche, connectez-vous en tant qu'administrateur.

Pour définir et activer un filtre d'interface, procédez comme suit :

1. S'il n'existe aucun profil de surveillance personnalisé pour les interfaces de surveillance, créez-en un ou copiez un profil pour créer un profil personnalisé. Vous ne pouvez pas modifier ou définir un filtre pour des profils de surveillance prédéfinis.
2. Sélectionnez un profil de surveillance d'interface personnalisé dans la page Profils de surveillance. Cliquez sur la ligne d'une famille de mesures d'interface à partir de l'onglet Familles de mesures, cliquez sur Modifier le filtre et modifiez les critères du filtre.

Remarque : Ne cliquez pas directement sur le nom de famille de mesures car il est lié de manière à vous donner directement accès à la définition de la famille de mesures. Cliquez plutôt sur la ligne contenant le nom de la famille de mesures pour activer l'option Modifier le filtre.

- Le champ Valeur de filtre est sensible à la casse.
- Pour les options Vitesse en entrée et Vitesse en sortie, vous pouvez entrer une valeur décimale en Mbit/s dans le champ de texte (1,544 par exemple).
- Pour plus d'informations sur la configuration du type, accédez au site Web d'iana : http://www.iana.org/assignments/ianaiftype-mib http://www.iana.org/assignments/ianaiftype-mib.

Lorsque vous enregistrez les modifications, les critères de filtre s'affichent dans l'onglet Familles de mesures.

3. Associez le profil de surveillance à une collection d'unités. (page 92)
4. Exécutez une détection (page 76), puis consultez le rapport de filtre dans la page Unités surveillées (page 99). Comparez les filtres sur chacun des autres profils de surveillance d'interface pour vérifier s'ils surveillent la même collection d'unités que celle que vous souhaitez filtrer.
5. Supprimez toute relation entre les autres profils de surveillance d'interface et les collections d'unités qui peuvent bloquer vos critères de filtre (page 92). Par exemple, vous pouvez associer le profil de surveillance d'interface avec la collection d'unités All Routers (Tous les routeurs). Dans ce cas, supprimez la relation entre les *autres* profils de surveillance d'interface et la collection d'unités All Routers.
6. Révisez le rapport de filtre mis à jour pour vérifier que les nouveaux critères de filtre sont actifs. Si le rapport de filtre indique qu'un profil de surveillance superflu a été inclus, répétez les étapes précédentes. Finalement, aucun profil de surveillance superflu n'est inclus et vous surveillez uniquement les interfaces qui doivent être surveillées.

Suppression d'un filtre d'interface

Vous pouvez utiliser des filtres d'interface avec des profils de surveillance personnalisés pour réduire le nombre d'interfaces surveillées. Vous pouvez effacer un filtre d'interface lorsque vous souhaitez collecter des données pour toutes les collections d'unités associées à un profil de surveillance personnalisé.

Remarque : Pour pouvoir effectuer cette tâche, connectez-vous en tant qu'administrateur.

Procédez comme suit :

1. Accédez à la liste de profils de surveillance.
2. Sélectionnez un profil de surveillance personnalisé qui surveille des interfaces réseau dans la liste.

   L'onglet Familles de mesures se remplit.
3. Sélectionnez une famille de mesures Interface et cliquez sur Effacer le filtre.

   Remarque : Cette option est activée uniquement lorsque vous sélectionnez une famille de mesures Interface pour laquelle un filtre est défini.

   Une boîte de dialogue de confirmation s'ouvre.
4. Cliquez sur Yes (Oui).

   Vos modifications sont enregistrées et le statut du filtre affiche un astérisque (*) dans l'onglet Familles de mesures pour indiquer qu'aucun filtre n'est défini. Le filtre est appliqué à la détection planifiée suivante (ou vous pouvez exécuter manuellement une détection).

Informations complémentaires :

Affichage des unités surveillées (page 99)

Convention d'attribution de nom de composants d'interface

La convention d'attribution de nom pour les composants d'interface approuvés par les certifications de fournisseur d'interfaces ou de fournisseur d'interfaces HSSI utilise la logique suivante :

- Si l'attribut ifName existe et contient une valeur, l'interface utilise cette valeur pour le nom.
- Si l'attribut ifName *n'existe pas* ou *ne contient aucune* valeur, l'interface utilise la valeur ifDescr pour le nom.

Remarque : Les nouvelles certifications pour la famille de mesures d'interface peuvent fournir une autre expression pour le nom d'interface.

Calcul de l'utilisation de l'interface

Data Aggregator permet de remplacer la valeur de la vitesse d'entrée et de la vitesse de sortie d'une interface pour garantir la précision des calculs. Par exemple, vous pouvez utiliser la commande de bande passante pour configurer ifSpeedIn et ifSpeedOut sur les interfaces de routeur pour affecter des décisions de routage. Dans ce cas, indiquez une vitesse de substitution avec Data Aggregator pour garantir que l'utilisation est calculée correctement.

Les paramètres que vous définissez au niveau de l'unité peuvent entraîner l'utilisation d'un débit de données supérieur ou inférieur au débit de données réel. En d'autres termes, la modification de la bande passante peut se traduire par des calculs de l'utilisation incorrects pour l'interface. Pour garantir le calcul correct de l'utilisation d'une interface, entrez une vitesse de substitution pour l'interface dans Data Aggregator.

Remplacement des valeurs de vitesse en entrée et de vitesse en sortie au niveau des interfaces

Par défaut, l'utilisation est calculée à l'aide des valeurs de vitesse d'entrée et de sortie spécifiées par l'unité (à laquelle l'interface appartient). Toutefois, vous pouvez remplacer la valeur de ces vitesses. Cela peut permettre une évaluation plus précise de l'utilisation de l'interface.

Procédez comme suit :

1. Cliquez sur Unités surveillées dans le menu Inventaire surveillé d'une source de données de Data Aggregator.

   L'onglet Arborescence s'affiche.

2. Dans la liste déroulante, sélectionnez Unité par collection ou Unité par profil de surveillance. Sélectionnez l'unité pour laquelle vous souhaitez remplacer les valeurs de vitesse en entrée et de vitesse en sortie d'une interface et sélectionnez la famille de mesures d'interface appropriée dans l'onglet Familles de mesures interrogées.

   Les composants d'interface qui sont surveillés au niveau de l'unité apparaissent dans le tableau Composants d'interface.

3. Sélectionnez le composant d'interface pour lequel vous souhaitez remplacer les valeurs de vitesse en entrée et en sortie et cliquez sur Modifier.

   La boîte de dialogue Modifier l'interface s'affiche. La boîte de dialogue affiche les valeurs de vitesse en entrée et en sortie détectées par défaut.

4. Entrez les valeurs de vitesse en entrée et de vitesse en sortie en bits par seconde et cliquez sur Enregistrer.

   Remarque : Vous pouvez cliquer sur Effacer et sur Enregistrer pour supprimer des substitutions. Les valeurs de vitesse spécifiées par l'unité sont alors utilisées dans les graphiques d'utilisation de la bande passante dans CA Performance Center pour l'interface. Un événement est généré au niveau de l'interface et indique que les substitutions de vitesse ont été supprimées. L'événement apparaît dans le tableau de bord Affichage des événements de CA Performance Center.

   La boîte de dialogue se ferme. Les valeurs de vitesse en entrée et de vitesse en sortie qui ont été remplacées dans l'interface sont signalées à l'aide d'un astérisque dans le tableau des composants d'interface.

   Un événement est généré au niveau de l'interface et indique que la valeur des vitesses d'entrée et de sortie a été remplacée. L'événement apparaît dans le tableau de bord Affichage des événements de CA Performance Center.

   Les valeurs de vitesse spécifiées sont alors utilisées dans les graphiques d'utilisation de la bande passante dans CA Performance Center pour l'interface.

Chapitre 6: Génération d'événements

Ce chapitre traite des sujets suivants :

Instructions concernant les performances des événements (page 135)
Evénements de gestion des performances (page 138)
Références moyennes (page 138)
Procédure de surveillance des performances d'unité à l'aide d'événements (page 139)
Surveillance des mesures à l'aide de règles d'événement (page 141)
Affichage des événements (page 149)
Procédure de configuration des notifications à partir du gestionnaire d'événements (page 150)

Instructions concernant les performances des événements

La configuration suivante a été utilisée pour valider et tester les performances des événements :

- Un système conforme aux spécifications recommandées pour un système de production de taille moyenne de 500 000 éléments interrogés (voir spécifications de dimensionnement de système).
- 10 règles d'événement, réparties dans 7 profils de surveillance et utilisées pour les éléments interrogés.
  - 1 règle d'événement a été évaluée à un taux de 1 minute sur une famille de mesures comprenant 33 pour cent des éléments interrogés.
  - 1 règle d'événement a été évaluée à un taux de 15 minutes sur une famille de mesures comprenant 33 pour cent des éléments interrogés.
  - Les règles restantes ont été appliquées à une portion des éléments restants interrogée à un taux de 5 minutes.
  - Les règles d'événement ont été réparties de façon équitable dans 4 familles de mesures.
  - Chaque règle possédait 1 condition fixe et 1 condition d'écart type.
  - 6 règles d'événement avec une durée de 5 minutes et fenêtre de 15 minutes.
  - 4 règles d'événement avec une durée de 5 minutes et fenêtre de 60 minutes.

  Remarque : Pour des performances optimales, réduisez le nombre de profils de surveillance qui ont des règles d'événement pour la même famille de mesures. Par exemple, un profil de surveillance avec dix règles pour la famille de mesures Interfaces fonctionnera mieux que dix profils de surveillance avec une règle pour la famille de mesures Interfaces, lorsqu'il est appliqué au même ensemble d'unités.

- Un nombre variable de règles d'événement étaient associées à 100 000 éléments interrogés.
- 5 systèmes Data Collector étaient utilisés, chacun interrogeant environ 1/5ème des éléments.

Méthode de surveillance du traitement des événements

Pour déterminer si le nombre d'événements surveillés est trop élevé, vous devez surveiller certains indicateurs clés de performance dans Data Aggregator. La surveillance d'événements dans Data Aggregator s'effectue par lots (des événements sont évalués et générés simultanément pour les grands groupes d'éléments par exemple). Nous avons donc utilisé une variété de mesures qui étaient suivies par le biais du mécanisme d'auto-surveillance du système Data Aggregator pour évaluer l'intégrité du système Data Aggregator. Pour afficher ces importantes mesures, ajoutez une vue multitendance d'unité IM personnalisée dans un tableau de bord. Modifiez le tableau de bord pour utiliser les mesures suivantes à partir de la famille de mesures **Nombre de calculs d'événements de Data Aggregator** :

- **Taille de la file d'attente des processus d'événement** : indique la taille de la file d'attente de traitement des événements. Une valeur de constante de zéro, un, ou deux indique que l'intégrité de ce système est correcte et qu'il peut maintenir le taux actuel de traitement d'événements. Une valeur de constante de plus de 2 indique que le système est en mesure de garantir les charges actuelles de traitement d'événements, mais qu'il est peut-être en retard (et qu'il traite des interrogations antérieures au cycle d'interrogation actuel). Une augmentation de la taille de la file d'attente sans récupération ultérieure (tendance descendante) indique que le traitement d'événements est sauvegardé et que votre système est peut-être en danger.
- Les deux mesures suivantes se complètent.
  - **Nombre d'événements effacés** : nombre d'événements effacés dans la fenêtre de résolution de génération de rapports.
  - **Nombre d'événements effacés** : nombre d'événements déclenchés dans la fenêtre de résolution de génération de rapports.

  Un nombre toujours supérieur aux événements déclenchés ou effacés peut avoir un impact sur la base de données du gestionnaire d'événements.

  Si le total combiné de ces deux mesures dépasse 900 événements pendant un cycle d'interrogation de 5 minutes, cela signifie que vous avez dépassé le taux de génération recommandé de 2-3 événements par seconde pour les systèmes de taille moyenne. La génération/suppression d'événements en rafale pour les 900 événements dans un cycle d'interrogation de 5 minutes est acceptable.

- **Evaluations de règles d'événement traitées** : une évaluation de règle d'événement est l'évaluation d'une règle d'événement unique d'après un élément unique. Cette mesure suit la somme des règles d'événement, multipliée par le nombre d'éléments auquel ces règles sont appliquées. Plus le nombre d'évaluations est élevé, plus votre système est chargé. Toutefois, les évaluations ne sont pas créées de la même façon. Par exemple, les évaluations avec plus de conditions, plus de conditions d'écart type, ou d'une durée supérieure et avec une fenêtre plus grande sont plus chères que les évaluations utilisant des conditions moins nombreuses et fixes d'une durée et avec une fenêtre inférieures. Le nombre d'évaluations que vous serez en mesure de réaliser variera selon vos règles d'événement.

  Dans notre environnement de test (décrit préalablement), nous avons constaté que le dépassement de 150 000 évaluations pendant un cycle d'interrogation de 5 minutes met le système en danger.

- **Temps total de calcul des événements** : durée totale du traitement des événements pour cette famille de mesures. Si ce nombre dépasse le nombre de secondes de la fenêtre de résolution de génération de rapports, cela indique que le traitement des événements a été retardé à ce moment.

La surveillance de toutes ces mesures sur une durée prolongée vous permet de connaître l'intégrité des performances d'événements sur votre système. En outre, si le journal Karaf sur le système Data Aggregator contient une erreur de base de données et/ou autre, cela peut indiquer que le système est surchargé. En général, ces mesures auto-surveillées doivent être régulières. Toutefois, en soirée (par défaut entre 02 h 00 et 4 h 00 UTC), certains jobs intensifs de base de données sont exécutés et peuvent entraîner des fluctuations dans les mesures auto-surveillées. Si les mesures reviennent à un état régulier, vous pouvez considérer que l'intégrité du système est satisfaisante (bien que les événements puissent être retardés lorsque le système est occupé).

Nous vous recommandons d'activer la génération d'événements de façon progressive et de vérifier l'intégrité du système avant de passer à des règles différentes. Nous vous recommandons également de surveiller l'intégrité du système pendant 24 heures après chaque modification ultérieure, car certains processus nocturnes peuvent avoir un impact même lorsque le traitement d'événements semble régulier pendant toutes les heures diurnes.

Méthode de correction en cas de dépassement du seuil

Pour corriger le dépassement d'un seuil, procédez comme suit :

1. Désactivez les règles d'événement individuellement. Vérifiez les performances après avoir désactivé chaque règle et avant d'en désactiver une autre.
2. Réduisez le nombre d'éléments interrogés.
3. Réduisez le nombre de profils de surveillance avec des règles d'événement qui interrogent des éléments.
4. Si ces étapes n'améliorent pas les performances, contactez le support CA.

Evénements de gestion des performances

Vous pouvez définir deux types d'événements de gestion des performances à l'aide de règles d'événement. Vous pouvez ajouter des règles d'événement aux profils de surveillance personnalisés.

Evénement avec dépassement de seuil

Déclenché par une règle constante (valeur fixe) lorsqu'une mesure observée diffère d'une définition corrigée de la valeur pendant une durée spécifiée pour une fenêtre de temps.

Exemple :

Vous pouvez définir une règle d'événement pour générer un événement lorsque l'utilisation de la bande passante dépasse 80 % pour une durée de 5 minutes et une fenêtre de 10 minutes lors d'une interrogation à un intervalle de 5 minutes.

Evénement d'écart par rapport à la normale

Déclenché par une règle d'écart type lorsqu'une mesure diffère de la mesure de base pour une durée et une fenêtre de temps spécifiées. La norme se base sur le calcul de la moyenne de référence. Initialement, lorsque des informations limitées ont été collectées, la moyenne de référence est calculée pour la même heure, chaque jour. Lorsque des données supplémentaires sont disponibles, Data Aggregator bascule ses calculs de moyenne sur une moyenne de type même heure, même jour de la semaine.

Exemple :

Vous pouvez définir une règle d'événement pour générer un événement lorsque l'utilisation de la bande passante dépasse de 1 écart type la moyenne horaire calculée pour le même jour de la semaine et la même heure, pour une durée de 5 minutes dans une fenêtre de 10 minutes lors de l'interrogation à un intervalle de 5 minutes.

Références moyennes

Selon la quantité des données interrogées qui sont collectées, les *moyennes de référence* sont calculées de deux façons :

- Initialement, la moyenne des moyennes horaires pour la même heure est calculée (indépendamment du jour).
- Une fois qu'un nombre suffisant de données est collecté, la moyenne des moyennes horaires même jour, même heure est calculée.

Les moyennes de référence permettent d'indiquer les performances pour les mesures surveillées sélectionnées et d'évaluer des performances actuelles. Les références moyennes et les écarts types associés sont calculés toutes les heures de manière continue. L'écart type fournit un indicateur statistique du degré de variabilité qui existe au niveau des données de remplissage qui interviennent dans le calcul de la référence moyenne.

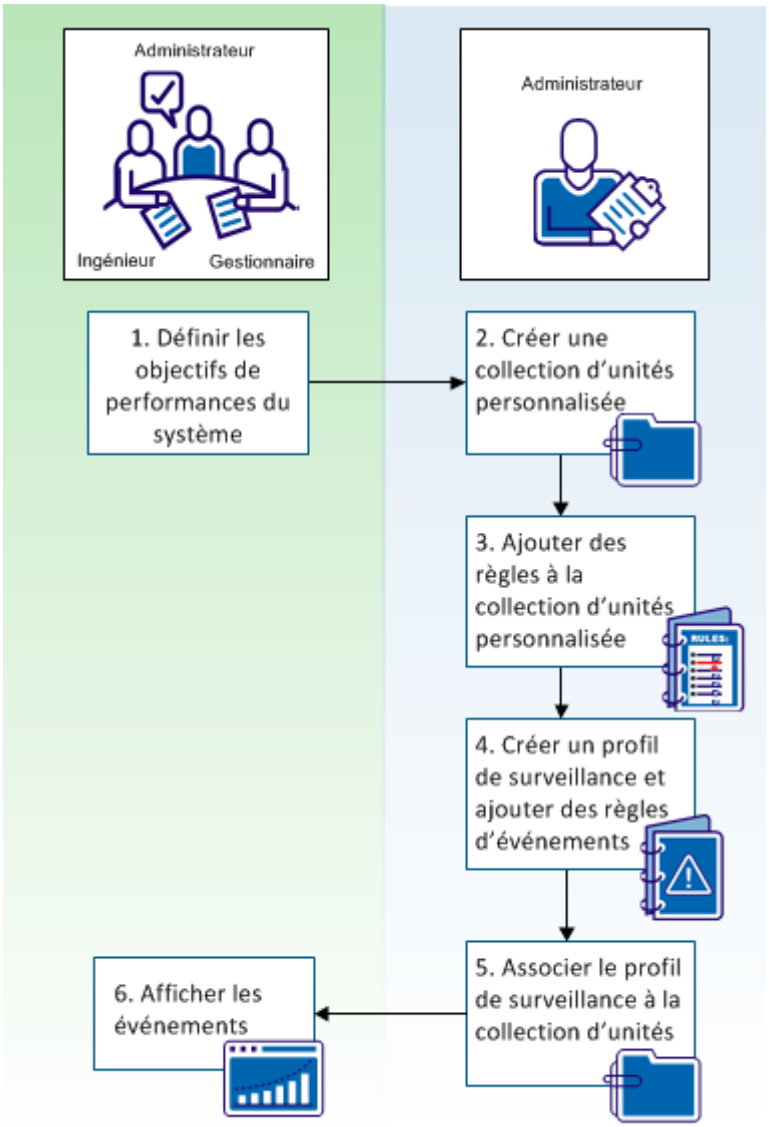
Dans Data Aggregator, la valeur de base pour une durée spécifiée dans une fenêtre de temps correspond à la moyenne de référence calculée.

Procédure de surveillance des performances d'unité à l'aide d'événements

Les gestionnaires (tels que le gestionnaire du centre d'opérations) et les ingénieurs (tels que les opérateurs informatiques ou les architectes informatiques) doivent pouvoir accéder, à tout moment, à des informations actualisées concernant l'intégrité de leurs systèmes. Ils collaborent avec l'administrateur d'outils pour configurer Data Aggregator dans le cadre de la génération des événements concernant des unités dont les performances s'éloignent de la normale. Ces événements permettent aux gestionnaires et aux architectes de surveiller proactivement l'intégrité de leur réseau et de corriger les problèmes de performance, si nécessaire.

Par exemple, votre organisation a récemment virtualisé plusieurs applications critiques pour l'entreprise afin d'améliorer l'efficacité. L'architecte informatique et le gestionnaire de centre d'opérations veulent surveiller ces serveurs virtuels pour être sûrs qu'ils peuvent gérer la charge à partir de ces applications. L'administrateur d'outils crée un profil de surveillance et ajoute des règles d'événement permettant de détecter les problèmes de surutilisation des unités centrales et de la mémoire virtuelle pour la collection d'unités virtuelles. Data Aggregator évalue automatiquement toutes les unités dans la collection après chaque interrogation pour chaque unité. Si nécessaire, Data Aggregator crée et efface des événements lorsque les unités remplissent les critères des règles d'événements.

L'illustration suivante affiche la procédure de génération des événements pour vous aider à surveiller les problèmes de performances d'unité de manière automatique :



Comme l'indique l'illustration, l'administrateur de d'outils collabore avec les ingénieurs et les gestionnaires pour définir les performances attendues d'un ensemble d'unités. L'administrateur décide ensuite de créer une collection d'unités personnalisée, de créer un profil de surveillance et d'affecter des règles d'événement au profil de surveillance. Pour lancer la surveillance des unités, l'administrateur associe le profil de surveillance, ainsi que ses règles d'événement affectées, à la collection d'unités personnalisée. L'administrateur, les ingénieurs et les gestionnaires peuvent afficher les événements dans CA Performance Center au fur et à mesure de leur génération.

Procédures
Création d'une collection d'unités personnalisée (page 142)
Ajout de règles à une collection d'unités personnalisée (page 143)
Création d'un profil de surveillance et ajout de règles d'événement (page 144)
Affectation d'un profil de surveillance à une collection d'unités personnalisée (page 148)
Affichage des événements (page 149).

Surveillance des mesures à l'aide de règles d'événement

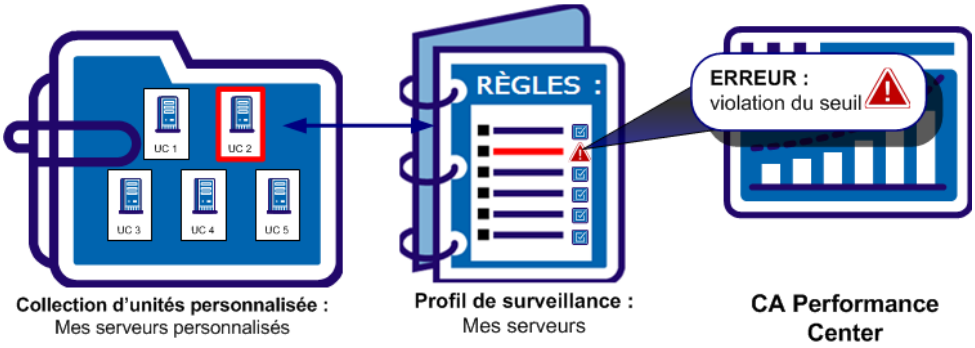
Les événements fournissent des informations utiles pour surveiller l'intégrité et le statut de votre environnement de réseau. De plus, l'intégration à CA Spectrum vous permet d'utiliser des événements pour automatiser des processus basés sur les données d'un message d'événement.

Data Aggregator utilise des profils de surveillance pour gérer les événements. Les profils de surveillance contiennent un ensemble de règles d'événement. Grâce aux mesures (à partir de vos familles de mesures), ces règles définissent les conditions que vous souhaitez surveiller.

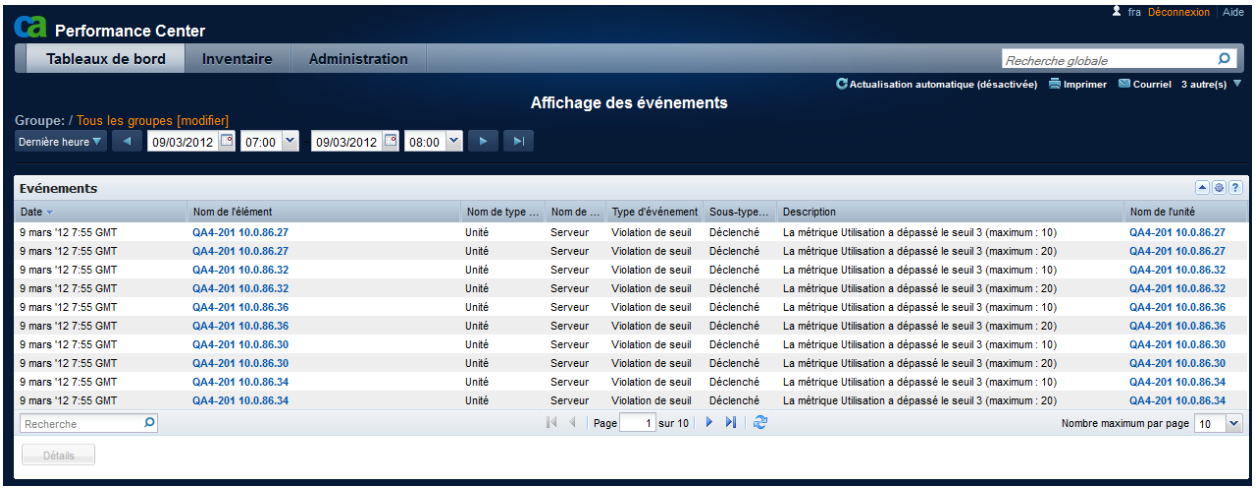
Pour implémenter les règles d'événement, associez le profil de surveillance à une collection d'unités.

Important : *Les collections d'unités sont primordiales pour le démarrage et l'arrêt du processus de surveillance*. Data Aggregator ne peut pas utiliser de profil de surveillance, sauf si vous l'associez à une ou plusieurs collections.

Data Aggregator applique immédiatement les règles de ce profil aux unités incluses dans cette collection. Grâce aux valeurs de mesures interrogées pour ces unités, les règles déclenchent et effacent les événements nécessaires.



Les événements apparaissent dans un tableau de bord CA Performance Center.



Remarque : Vous pouvez générer des alarmes visibles par l'utilisateur dans CA Spectrum à partir d'événements qui sont traités et qui sont journalisés dans Data Aggregator. Pour plus d'informations, reportez-vous à la documentation de CA Spectrum.

Création d'une collection d'unités personnalisée

En tant qu'administrateur d'outils de Data Aggregator, vous recevez une demande de surveillance des performances d'un nouveau groupe de serveurs virtuels. L'architecte informatique et le responsable du centre opérationnel souhaitent effectuer le suivi de l'utilisation de l'UC et de la mémoire. Ces serveurs virtuels hébergent des applications critiques, ils veulent donc des mises à jour fréquentes sur leur statut.

Remarque : Nous partons du principe que vous avez déjà exécuté une détection initiale sur votre réseau et que vous avez détecté une partie des serveurs virtuels.

Vous décidez de créer d'abord une collection d'unités personnalisée pour grouper les serveurs virtuels détectés, car aucune collection d'unités prédéfinie (prête à l'emploi) n'est disponible pour les serveurs virtuels. Pour créer une collection d'unités personnalisée, créez d'abord une collection d'unités personnalisée dans CA Performance Center. La synchronisation automatique crée une collection d'unités correspondante dans Data Aggregator.

Procédez comme suit :

1. Connectez-vous à CA Performance Center en tant qu'utilisateur avec le rôle d'administrateur.
2. Sélectionnez Administration, Paramètres personnalisés, puis Groupes.

   La boîte de dialogue Gérer les groupes s'ouvre.

3. Cliquez avec le bouton droit de la souris sur Collection gérée, puis sélectionnez Ajouter un nouveau groupe.

   La boîte de dialogue Ajouter un nouveau groupe s'affiche. L'onglet Créer est sélectionné par défaut.

4. Fournissez des valeurs pour les paramètres suivants :

   Nom du groupe

   Spécifie un nom pour le groupe. Pour cet exemple, nommez le groupe Serveurs virtuels.

   Remarque : N'utilisez pas les caractères spéciaux suivants dans les noms de groupe : /&\,%.

   Description

   (Facultatif) Vous aide à identifier le groupe.

5. Cliquez sur Enregistrer.

   Le groupe Serveurs virtuels apparaît dans l'arborescence de groupes Surveillé. Patientez jusqu'au lancement de la synchronisation automatique avec Data Aggregator. Lors de la synchronisation, Data Aggregator crée les collections d'unités correspondantes à utiliser pour la surveillance des unités. La synchronisation peut ne commencer qu'au bout de cinq minutes.

Ajout de règles à une collection d'unités personnalisée

Les réseaux et les systèmes évoluent constamment. Les collections d'unités sont automatiquement mises à jour pour inclure les unités dès leur détection. Toutefois, la mise à jour des collections d'unités personnalisées peut s'avérer difficile. C'est pourquoi, vous pouvez utiliser des règles pour ajouter les collections d'unités personnalisées. Les éléments nouvellement détectés qui répondent aux spécifications des règles sont ajoutés aux collections d'unités. De même, les unités sont supprimées si elles ne répondent pas aux exigences de règle ou qu'elles ne sont plus surveillées.

Vous pouvez ajouter des règles de groupe à des groupes pour remplir et mettre à jour automatiquement un contenu de groupe en fonction de différentes conditions. Dans ce cas, vous voulez ajouter des règles de groupe à la collection d'unités personnalisée Virtual Servers (Serveurs virtuels) pour l'actualiser avec les serveurs virtuels détectés. Pour ce scénario, nous partons du principe que les adresses IP des ordinateurs virtuels sont compris dans une plage donnée.

Procédez comme suit :

1. Dans le menu principal de CA Performance Center, sélectionnez Administration, Paramètres personnalisés, puis cliquez sur Groupes.

   La boîte de dialogue Gérer les groupes s'ouvre.

2. Sélectionnez le groupe que vous souhaitez remplir dans l'arborescence Groupes.

   Remarque : Les unités qui sont ajoutées directement à un groupe lors d'une étape manuelle apparaissent comme des éléments directs dans le volet Propriétés de groupe. Les composants qui sont ajoutés à un groupe parce qu'ils sont des enfants d'une unité gérée sont des éléments hérités dans les Propriétés de groupe.

3. Cliquez sur l'onglet Règles, puis sur Ajouter une règle.

   La boîte de dialogue Ajouter une règle s'ouvre.

4. Attribuez un nom à la règle dans le champ Nom de la règle.

5. Dans la liste Ajouter, sélectionnez Unités.

6. Cliquez sur Ajouter une condition.

   Une ligne de listes déroulantes et de champs s'affiche.

7. Procédez comme suit :

   - Dans la première liste, sélectionnez Adresse de l'unité.
   - Dans la deuxième liste, Sélectionnez la méthode de correspondance "est entre".
   - Dans la troisième liste, entrez DE a*dresse IP de début* A *adresse IP de fin* pour indiquer la plage de détection des adresses IP des ordinateurs virtuels.

8. Cliquez sur Résultats de l'aperçu pour confirmer que la nouvelle règle comprend les unités de votre choix.

   Les résultats s'affichent dans la fenêtre Aperçu des règles de groupe. Vous pouvez développer chaque type d'unité pour connaître les unités qui sont ajoutées.

9. Cliquez sur Enregistrer ou sur Enregistrer et exécuter les règles :

   - Enregistrement : enregistre les règles sans exécuter les règles. Le groupe est rempli pendant la synchronisation globale suivante, qui se produit environ toutes les 5 minutes.
   - Enregistrer et exécuter les règles : enregistre les règles et remplit le groupe immédiatement.

Création d'un profil de surveillance et ajout de règles d'événement

Pour configurer le processus de surveillance des performances des serveurs virtuels dans votre collection groupe personnalisée Virtual Servers (Serveurs virtuels), vous devez d'abord créer un profil de surveillance, puis ajouter des règles d'événement à ce profil de surveillance.

Les règles d'événement ne sont pas incluses dans les profils de surveillance prédéfinis (prêt à l'emploi) et vous ne pouvez pas modifier ces profils afin d'ajouter des règles d'événement. Vous copiez un profil de surveillance existant pour utiliser comme base de la création d'un profil similaire en y apportant quelques modifications. Les modifications que vous apporterez au profil de surveillance personnalisé constitueront à ajouter des règles d'événement.

Suite à la collaboration avec l'architecte informatique et le gestionnaire du centre d'opérations, vous décidez de créer un profil de surveillance et d'ajouter les règles d'événement suivantes :

- Ajoutez une règle d'utilisation de mémoire VMware, comme suit :
  - Une violation se produit lorsque l'utilisation de mémoire dépasse 80 % pendant 300 secondes (5 minutes) dans une fenêtre de 900 secondes (15 minutes).
  - Effacez la violation lorsque l'utilisation de la mémoire est égale ou inférieure à 75 % pendant 300 secondes dans une fenêtre de 900 secondes.
- Ajoutez une règle d'utilisation d'UC de VMware, comme suit :
  - Une violation se produit lorsque les *deux* conditions suivantes sont remplies :
    - Condition 1 : l'utilisation de l'UC est supérieure à 70 %.
    - Condition 2 : l'utilisation de l'UC est supérieure à un écart type.
  - Ces conditions se produisent pendant 300 secondes dans une fenêtre de 900 secondes.

Procédez comme suit :

1. Sélectionnez Administration, Paramètres de source de données, puis cliquez sur une source de données de Data Aggregator.
2. Dans la page d'administration de Data Aggregator, accédez au menu Configuration de la surveillance et cliquez sur Profils de surveillance.

   Une liste de profils de surveillance est remplie.
3. Sélectionnez le profil de surveillance Serveur virtuel et cliquez sur Copier.

   La boîte de dialogue Créer/modifier un profil de surveillance s'ouvre.
4. Définissez le nom du profil de surveillance sur Serveurs virtuels personnalisés.
5. Cliquez sur Enregistrer.

   Le profil de surveillance que vous avez copié est ajouté à la liste Profils de surveillance.
6. Sélectionnez le profil de surveillance Serveurs virtuels personnalisés.
7. Cliquez sur l'onglet Règles d'événement.
8. Créez la règle d'événements d'utilisation de mémoire VMware comme suit :
   a. Cliquez sur Créer.

b. Entrez les valeurs suivantes pour votre nouvelle règle d'événements :

- **Nom :** VirtualMemUsageTooHigh
- **Description** (facultatif) : utilisation de la mémoire VMware
- **Famille de mesures :** ordinateur virtuel VMware
- **Durée :** 300

  Remarque : Dans cet exemple, les unités sont interrogées à un intervalle par défaut de 300 secondes. La valeur de durée est utilisée pour les seuils de violation et d'effacement.
- **Fenêtre :** 900

  Remarque : La valeur de fenêtre est utilisée pour les seuils de violation et d'effacement.
- **Sévérité :** majeure

c. Dans la section Une violation se produit lorsque toutes ces conditions sont remplies, sélectionnez les valeurs suivantes :

- **Mesure :** utilisation de la mémoire de l'ordinateur virtuel
- **Opérateur :** Au-dessus
- **Valeur :** 80
- **Type de condition :** Valeur fixe

d. Dans la section Une violation est effacée lorsque, sélectionnez les valeurs suivantes :

- **Opérateur :** Egal ou inférieur à
- **Valeur :** 75

e. Cliquez sur Enregistrer.

9. Cliquez sur l'onglet Règles d'événement.
10. Créez la règle d'événements d'utilisation d'UC de VMware en utilisant plusieurs conditions, de la façon suivante :

a. Cliquez sur Créer dans la zone de groupe Règles d'événement.

b. Entrez les valeurs suivantes pour votre nouvelle règle d'événements :

- **Nom :** VMwareCpuUtil
- **Description** (facultatif) : utilisation de l'UC VMware
- **Famille de mesures :** ordinateur virtuel VMware
- **Durée :** 300
- **Fenêtre :** 900
- **Sévérité :** majeure

c. Dans la section Une violation se produit lorsque toutes ces conditions sont remplies, sélectionnez les valeurs suivantes :

- **Mesure :** Utilisation de l'UC
- **Opérateur :** Au-dessus
- **Valeur :** 70
- **Type de condition :** Valeur fixe

d. Cliquez sur Ajouter une condition.

e. Dans la section Une violation se produit lorsque toutes ces conditions sont remplies, sélectionnez les valeurs suivantes :

- **Mesure :** Utilisation de l'UC
- **Opérateur :** Au-dessus
- **Valeur :** 1
- **Type de condition :** Ecart type

Remarque : Plusieurs règles d'événement de condition sont limitées aux mesures d'une famille de mesures spécifique. Dans cet exemple, la famille de mesures est déjà disponible pour l'utilisation dans Data Aggregator. Pour plus d'informations sur la création d'une famille de mesures personnalisée, consultez le *Manuel d'autocertification de Data Aggregator*.

Lorsque plusieurs conditions sont définies, l'événement d'effacement est généré lorsque plus aucune condition n'est vraie.

Important : Le calcul des références pour toutes les heures peut prendre 48 heures maximum à partir du lancement de la surveillance d'une famille de mesures pour Data Aggregator. Des données de référence sont requises pour les règles d'écart type.

11. Cliquez sur Enregistrer.

Vos règles d'événement sont enregistrées. Les règles d'événement sont filtrées par familles de mesures dans le profil de surveillance Serveurs virtuels personnalisés pour garantir l'évaluation de toutes les règles que vous définissez.

Affectation d'un profil de surveillance à une collection d'unités personnalisée

Vous avez créé le profil de surveillance Serveurs virtuels personnalisés et vous avez ajouté des règles d'événement pour surveiller les ordinateurs virtuels qui exécutent des applications métier critiques. Pour lancer la surveillance de vos unités virtuelles et pour activer des règles d'événement, affectez le profil de surveillance Mes serveurs virtuels à la collection d'unités personnalisée Virtual Servers (Serveurs virtuels).

Important : *Les collections d'unités sont primordiales pour le démarrage et l'arrêt du processus de surveillance*. Data Aggregator ne peut pas utiliser de profil de surveillance, sauf si vous l'associez à une ou plusieurs collections.

Procédez comme suit :

1. Dans la page d'administration de Data Aggregator, accédez au menu Configuration de la surveillance et cliquez sur Collections.

   Une liste de collections d'unités s'affiche.

2. Sélectionnez la collection d'unités Virtual Servers (Serveurs virtuels) et cliquez sur l'onglet Profils de surveillance.

   Une liste affiche les profils de surveillance qui sont assignés à la collection d'unités sélectionnée. Cette liste sera vide.

3. Cliquez sur Gérer.

   La boîte de dialogue Assigner des profils de surveillance de collection s'ouvre.

4. Dans la liste des profils de surveillance disponibles, sélectionnez le profil de surveillance Mes serveurs virtuels et cliquez sur Ajouter.

   Le profil de surveillance sélectionné est ajouté à la liste des profils de surveillance affectés.

5. Cliquez sur Enregistrer.

   Data Aggregator lance la surveillance de cette collection d'unités à l'aide de votre profil de surveillance et de vos règles d'événement. Les événements qui sont générés apparaissent dans le tableau de bord Affichage des événements.

Affichage des événements

CA Performance Center affiche des événements dans un rapport qui est appelé vue Evénements. Les événements les plus récents s'affichent d'abord. Vous pouvez contrôler le contenu du rapport d'événements pour afficher les données d'événement les plus pertinentes pour vous. Les fonctionnalités qui contrôlent le contenu de rapport incluent les contrôles d'heure et les fonctionnalités de tri et de filtre.

Exemples :

- **Suivi des changements de configuration :** lorsque vous ne sélectionnez *pas* l'option Mise à jour automatique des familles de mesures sur un profil de surveillance personnalisé, vous devez afficher le fichier journal d'événements pour consulter les changements de configuration et cliquer alors manuellement sur Mettre à jour la famille de mesures dans la vue Unités surveillées, Familles de mesures interrogées pour que Data Aggregator récupère bien la configuration d'unité.
- **Dépannage des problèmes de performance :** pour dépanner des problèmes de performance avec un serveur spécifique, vous pouvez filtrer les événements en fonction de l'adresse IP du serveur. La vue Evénements filtre la liste complète des événements pour afficher uniquement les événements pour le serveur sélectionné.

Pour afficher des événements, cliquer sur le menu Tableaux de bord dans CA Performance Center et, sous Affichages des opérations, sélectionnez Affichage des événements.

La vue Evénements s'ouvre. La table affiche les événements qui se sont produits dans la période sélectionnée, en répertoriant l'événement le plus récent d'abord.

Remarque : Pour plus d'informations sur les événements, reportez-vous au *Manuel de l'opérateur de CA Performance Center* et à l'Aide en ligne de CA Performance Center.

Procédure de configuration des notifications à partir du gestionnaire d'événements

Vous pouvez configurer la génération de notifications concernant les événements provenant de Data Aggregator et envoyés au gestionnaire d'événements. Les événements entrants sont évalués en fonction des conditions que vous configurez pour les critères de notification. Le gestionnaire d'événements envoie une action de notification uniquement lorsque les critères sont remplis. Si un événement ne déclenche pas de notification, vous pouvez afficher l'événement dans la liste d'événements.

Les types de notification suivants sont disponibles dans l'assistant de création/modification de notifications :

Interruption

Envoie des notifications par interruption au système de gestion de pannes ou de réseau (NMS) de votre environnement, tel que CA Spectrum. Ce type de notification prend en charge la spécification de plusieurs destinations. La première destination est requise.

Deux bases de données d'informations de gestion sont disponibles dans l'assistant de notifications afin de garantir la compatibilité avec les clients existants.

Rôles pris en charge : les utilisateurs avec le rôle Administrateur peuvent configurer des notifications d'interruption.

Courriel

Cette option permet d'envoyer des notifications par courriel à un ou à plusieurs destinataires lorsqu'un événement est généré ou activé. Le courriel contient un lien permettant d'afficher la page de contexte pour l'unité ou le composant ayant déclenché l'alarme.

Rôles pris en charge : les utilisateurs disposant du rôle Créer des notifications peuvent configurer des notifications par courriel.

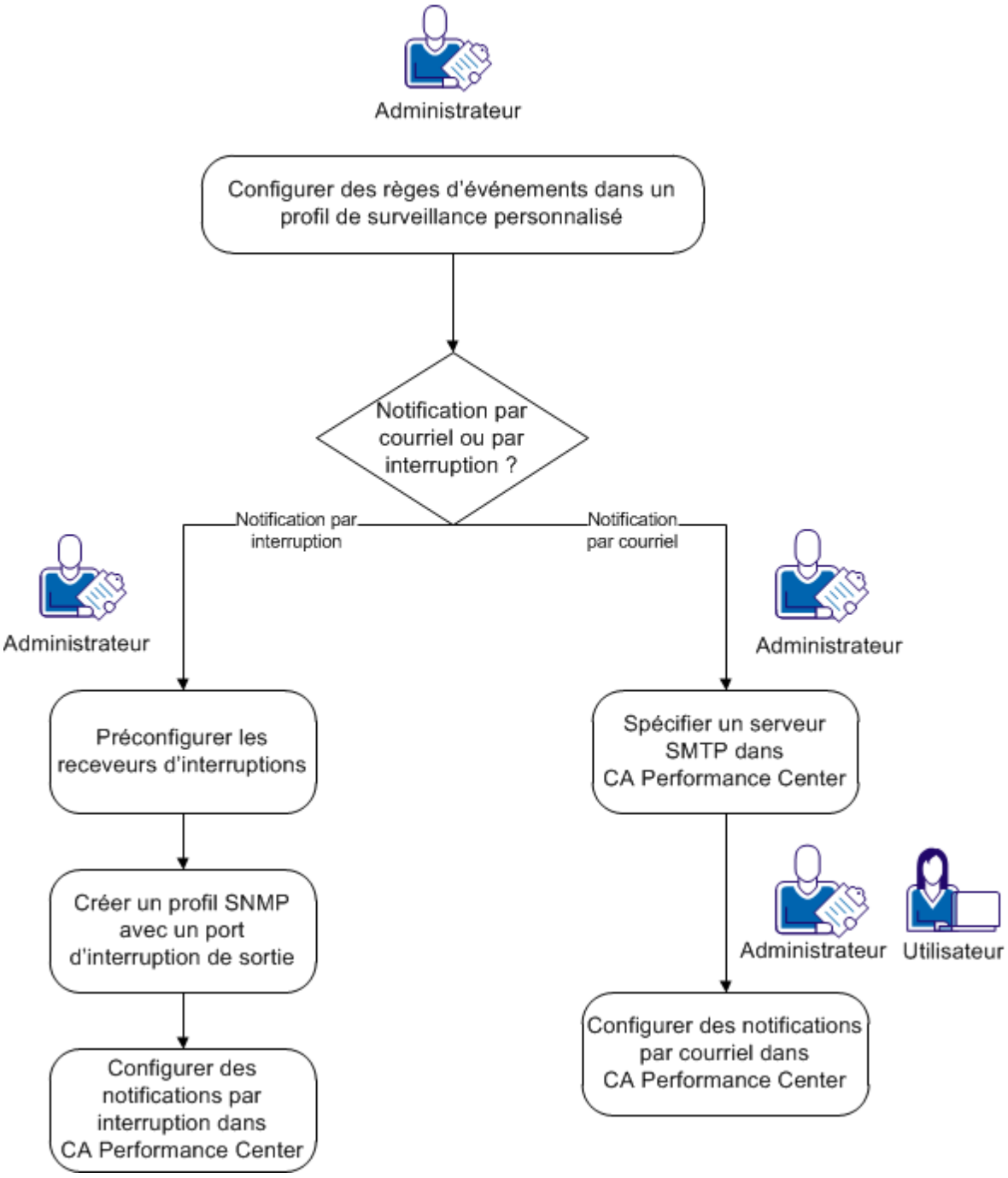
Un utilisateur configure et reçoit uniquement les notifications pour les événements relatifs à une unité appartenant à un groupe auquel il a accès.

Tenez compte des informations suivantes :

- Les notifications sont propres à l'utilisateur ; les utilisateurs ne peuvent pas afficher les notifications créées par d'autres utilisateurs.
- L'option Notifications s'affiche uniquement lorsque le gestionnaire d'événements est activé et indique l'état de synchronisation Disponible
- L'action de suppression des notifications d'événements n'affecte pas les événements réels ou futurs.

Le diagramme suivant indique les flux de travaux possibles pour les options de notification d'événement :

Flux de travaux de configuration de notification d'événements



Vous pouvez procéder comme ci-dessous pour configurer des interruptions ou des notifications par courriel :

1. Configurez les règles d'événement dans l'onglet Règles d'événement d'un profil de surveillance dans les pages d'administration de source de données Data Aggregator.
2. (Interruptions uniquement) Les récepteurs d'interruption doivent être préconfigurés pour la réception des interruptions. La communauté SNMP et la destination IPV4 peuvent être uniques pour chaque destination. Pour plus d'informations sur les formats des interruptions, consultez la documentation concernant le système NMS correspondant à votre récepteur d'interruptions.
3. (Interruptions uniquement) Créez un profil SNMP avec le port d'interruption sortant (port 162 généralement) avant de créer la notification.
4. (Messagerie électronique uniquement) Configurez les paramètres de serveur SMTP en sélectionnant Serveur de messagerie dans Administration, puis dans le menu de Paramètres du système dans CA Performance Center.
5. Effectuez l'*une* des actions suivantes :
   - (Administrateurs) Créez une notification en sélectionnant Administrateur, Notifications dans CA Performance Center. Pour les notifications d'interruption, sélectionnez le profil SNMP que vous avez créé à l'étape 2.

     Remarque : En tant qu'administrateur de clients hébergés par défaut, vous pouvez créer une notification pour un administrateur de clients hébergés ou pour un utilisateur de client hébergé, en vous situant dans un contexte d'utilisateur réel. Connectez-vous en tant qu'administrateur de clients hébergés ou en tant qu'utilisateur de client hébergé. De même, l'administrateur de clients hébergés par défaut peut administrer le client hébergé et déléguer à l'utilisateur la création d'une notification limitée aux clients hébergés.
   - (Utilisateurs) Créez des notifications par courriel en sélectionnant Mes paramètres, puis Notifications dans CA Performance Center.

   Remarque : Les administrateurs peuvent également utiliser l'API du gestionnaire d'événements pour gérer les notifications. Entrez l'URL ci-dessous pour accéder à l'interface autodocumentée de l'hôte du gestionnaire d'événements : http://*nom_hôte*:8281/EventManager/webservice/notifications/documentation.

Types d'événements

Chaque événement créé dans CA Infrastructure Management inclut le type d'événement et les éventuelles informations de sous-type d'événement. Ces informations aident CA Infrastructure Management à traiter correctement les événements pour vous maintenir informé du statut et de l'intégrité de votre infrastructure.

Les types d'événement standard fournis dans CA Infrastructure Management sont les suivants :

- Evénement d'interrogation : s'applique à des événements qui résultent de l'interrogation ou de l'analyse de données d'interrogation.
- Evénement d'interruption : s'applique à des événements qui résultent des entrées d'interruption.
- Evénement de seuil : s'applique à des événements déclenchés par des violations de seuil au niveau de vos unités.
- Changement de reconfiguration : s'applique aux unités qui sont créées, détruites ou modifiées.
- Evénement inconnu : indique un événement de type inconnu.
- Tout : représente un type d'événement de caractère générique spécial qui signale aux abonnés tous les événements soumis au moteur d'événements.

Les types d'événement sont automatiquement affectés lors de la création d'événement. Toutefois, CA Infrastructure Management vous permet de définir des types d'événement personnalisés pour aider à gérer les événements de façon cohérente. A l'aide de types d'événement personnalisés, vous pouvez définir des familles d'événement qui s'appliquent à votre environnement unique de mise en réseau. Lorsque vous créez un type d'événement, vous déterminez les attributs requis pour ce type. Ainsi, tous les événements d'un type identique fournissent de façon cohérente les mêmes informations.

Après avoir créé les types d'événement personnalisés, vous pouvez configurer des règles de normalisation d'événement pour mapper ces événements bruts vers vos types d'événement personnalisés. Avec les événements normalisés, vous pouvez ignorer les différences entre les fournisseurs et les versions lorsque vous définissez le mode de traitement des événements. Par conséquent, CA Infrastructure Management peut traiter des événements normalisés pour satisfaire plus précisément vos besoins de gestion.

Remarque : Pour plus d'informations sur les éléments, reportez-vous au *Manuel de l'opérateur de CA Performance Center*.

Chapitre 7: Reporting

Ce chapitre traite des sujets suivants :

Utilisation des filtres (page 155)
Références moyennes (page 156)
95e centile (page 157)
Ecart type (page 157)
Valeurs minimum et maximum (page 158)

Utilisation des filtres

Vous pouvez utiliser des vues et des rapports dans un flux de travaux logique qui vous permet de voir l'entreprise entière pour identifier les problèmes, puis afficher la vue détaillée des unités et des composants pour isoler ces problèmes. Vous pouvez également accéder directement à des unités et à des composants quand vous savez déjà quel système ou quelle application dépanner. Vous pouvez également utiliser les informations des vues pour identifier de manière proactive des problèmes potentiels, pour la planification de la capacité et pour établir des rapports mensuels concernant l'intégrité du réseau.

Remarque : Il peut y avoir un retard entre l'interrogation des données et leur affichage dans les vues et les rapports. S'il y a une erreur de chargement des données, un message est enregistré dans le journal de l'unité Data Aggregator.

Les types suivants de vues et de rapports sont disponibles :

Tableaux de bord

Contient des ensembles de vues qui vous permettent de consulter les données interrogées comme informations explicites et de générer des rapports pour les principales unités à travers l'entreprise. Sélectionnez Tableaux de bord, puis sélectionnez un tableau de bord spécifique dans la liste pour ouvrir ce dernier. Vous pouvez explorer une unité, puis un composant d'unité si nécessaire.

Vues d'unité

Affichent des données interrogées comme un ensemble de vues par défaut pour une unité spécifiée. Accédez à un tableau de bord, ou sélectionnez Inventaire, Unités, puis une unité spécifique pour accéder aux vues contenant les données de cette dernière. Pour afficher les vues di contexte de l'unité dans les différentes catégories de performances, sélectionnez un onglet.

Vues de composant d'unité

Affichent plusieurs vues simultanément dans un rapport pour les composants d'unité. Accédez à la vue d'une unité, ou sélectionnez Inventaire, Composants d'unité, puis sélectionnez un composant pour afficher la page de ses composants.

Remarque : Pour plus d'informations sur la personnalisation des tableaux de bord et des vues, reportez-vous à l'aide en ligne de CA Performance Center.

Si les données ne s'affichent pas dans une vue, accédez directement à la page "Unités surveillées" à partir de la vue et procédez aux étapes ci-dessous de résolution du problème. Cliquez sur **Paramètres,** puis sur **Administrateur d'unités**. Cette option requiert les droits de rôle **Navigation à partir des vues dans la page d'administration de DA**, que vous pouvez affecter à l'utilisateur de votre choix. L'administrateur global possède ces droits de rôle par défaut.

Références moyennes

Selon la quantité des données interrogées qui sont collectées, les *moyennes de référence* sont calculées de deux façons :

- Initialement, la moyenne des moyennes horaires pour la même heure est calculée (indépendamment du jour).
- Une fois qu'un nombre suffisant de données est collecté, la moyenne des moyennes horaires même jour, même heure est calculée.

Les moyennes de référence permettent d'indiquer les performances pour les mesures surveillées sélectionnées et d'évaluer des performances actuelles. Les références moyennes et les écarts types associés sont calculés toutes les heures de manière continue. L'écart type fournit un indicateur statistique du degré de variabilité qui existe au niveau des données de remplissage qui interviennent dans le calcul de la référence moyenne.

Dans Data Aggregator, la valeur de base pour une durée spécifiée dans une fenêtre de temps correspond à la moyenne de référence calculée.

95e centile

Un centile est la valeur d'une variable regroupant un certain pourcentage d'observations. Par exemple, le 95e centile est la valeur (ou le score) sous lequel se situent 95 % des observations.

La surveillance du 95e centile se rapporte à la bande passante. Cette statistique est utile pour mesurer le débit de données car elle reflète de façon plus précise la capacité requise du lien surveillé pour les applications sensibles à la bande passante. Le 95e centile indique que 95 % du temps, l'utilisation de la bande passante est inférieure à cette quantité. Les 5 % de restants, l'utilisation de la bande passante est supérieure cette quantité. Si vous utilisez le 95e centile pour effectuer une planification de la capacité, nous recommandons de définir l'intervalle d'interrogation sur au moins 1 minute pour les unités surveillées.

Le 95e centile est calculé dans le cadre de cumuls et à des fins de génération de rapports.

Un *cumul* est le processus au cours duquel les valeurs de mesure sont cumulées. Dans un cumul horaire, les valeurs interrogées à la minute 1, la minute 5, à la minute 15, à la minute 30 et à la minute 60 pour les mesures sont cumulées toutes les heures. Dans un cumul quotidien, les valeurs horaires des mesures sont cumulées une fois par jour. Dans un cumul hebdomadaire, les valeurs quotidiennes des mesures sont cumulées une fois par semaine.

Ecart type

L'écart standard indique l'écart par rapport à la moyenne (valeur moyenne ou attendue). Un écart standard bas indique que les points de données tendent à être très proches de la moyenne. Un écart standard élevé indique que les points de données s'étendent sur une large plage de valeurs.

L'écart type est calculé pour des cumuls, des événements et à des fins de génération de rapports.

Un *cumul* est le processus au cours duquel les valeurs de mesure sont cumulées. Dans un cumul horaire, les valeurs interrogées à la minute 1, la minute 5, à la minute 15, à la minute 30 et à la minute 60 pour les mesures sont cumulées toutes les heures. Dans un cumul quotidien, les valeurs horaires des mesures sont cumulées une fois par jour. Dans un cumul hebdomadaire, les valeurs quotidiennes des mesures sont cumulées une fois par semaine.

Valeurs minimum et maximum

Les valeurs minimum et maximum sont calculées pour les cumuls et à des fins de génération de rapports. Ces valeurs permettent d'observer les limites de performance supérieure et inférieure au cours d'un intervalle de temps donné.

Un *cumul* est le processus au cours duquel les valeurs de mesure sont cumulées. Dans un cumul horaire, les valeurs interrogées à la minute 1, la minute 5, à la minute 15, à la minute 30 et à la minute 60 pour les mesures sont cumulées toutes les heures. Dans un cumul quotidien, les valeurs horaires des mesures sont cumulées une fois par jour. Dans un cumul hebdomadaire, les valeurs quotidiennes des mesures sont cumulées une fois par semaine.

Cumuls horaires :

- Minimum : la valeur minimum des valeurs interrogées.
- Maximum : la valeur maximum des valeurs interrogées.

Cumuls quotidiens :

- Minimum : la valeur minimum des minimums horaires.
- Maximum : la valeur maximum des maximums horaires.

Cumuls hebdomadaires et au-delà :

- Minimum : la valeur minimum des minimums quotidiens.
- Maximum : la valeur maximum des maximums quotidiens.

Génération de rapports de résolution de cinq minutes :

- Minimum : la valeur minimum des valeurs interrogées.
- Maximum : la valeur maximum des valeurs interrogées.

Génération de rapports de résolution horaires :

- Minimum : la valeur minimum des minimums horaires.
- Maximum : la valeur maximum des maximums horaires.

Génération de rapports de résolution quotidiens :

- Minimum : la valeur minimum des minimums quotidiens.
- Maximum : la valeur maximum des maximums quotidiens.

Annexe A: Calculs

Ce chapitre traite des sujets suivants :

Calculs de moyenne de référence (page 159)
Calculs du 95e centile (page 164)
Calculs d'écart standard (page 166)

Calculs de moyenne de référence

Initialement, lorsqu'un nombre limité de données est collecté, la référence moyenne est calculée pour la même heure de chaque jour précédent de la semaine. Par exemple, après deux jours de données d'historique collectées, une référence moyenne est calculée sur la période 09 h 00 - 10 h 00, en faisant la moyenne des cumuls horaires sur la même période, sur deux jours consécutifs.

Lorsque davantage de données sont disponibles, une permutation dans la méthode de calcul se produit automatiquement et Data Aggregator définit la norme en établissant la moyenne des échantillons horaires pour les mêmes jours de la semaine. Cette méthode tient alors compte des modèles de jour de la semaine dans l'utilisation. Cette méthode fournit une meilleure approximation de la valeur de base, qui peut entraîner une réduction du nombre de violations manquées et d'événements faux positifs générés. Par exemple, au bout de trois semaines de données d'historique collectées, une référence moyenne est calculée sur la période 09 h 00 - 10 h 00, en faisant la moyenne des cumuls horaires pour les trois lundis de cette période de trois semaines.

Remarque : Par défaut, cette permutation automatique se produit lorsqu'au moins 3 échantillons de données même heure, même jour de la semaine sont disponibles sur les 12 dernières semaines. Data Aggregator revient automatiquement à la méthode de calcul chaque jour, chaque heure, lorsque le nombre requis de points de données n'est plus disponible. Ces paramètres par défaut sont configurables. Pour plus d'informations sur la modification des paramètres par défaut, consultez le *Manuel des services Web REST de Data Aggregator*.

Les références moyennes sont calculées à des fins de génération d'événements et de rapports.

Exemple : calcul de la moyenne pour la même heure et de l'écart type de remplissage pour l'utilisation d'UC

L'exemple suivant indique la manière dont la moyenne pour la même heure et l'écart type de remplissage sont calculés pour l'utilisation d'UC sur une unité spécifique, avec trois points de données à 02 h 00 le lundi, mardi et mercredi.

Procédez comme suit :

1. Collectez 3 points de données.

   ```
   Jour :                              Lundi       Mardi      Mercredi

   Utilisation d'UC moyenne :    76           65           10
   ```

2. Calculez la moyenne de remplissage.

   La formule de calcul de la moyenne de remplissage est la suivante :

   ```
   La moyenne de remplissage = somme des valeurs de point de données dans le
   remplissage/nombre de points de données.
   ```

   L'équation pour cet exemple est la suivante :

   ```
   (76+65+10)/3

   La moyenne de remplissage = 50,33
   ```

3. Calculez la différence entre chaque point de données et la moyenne.

   Les différences pour cet exemple sont les suivantes :

   ```
   25.67    14.67    -40.33
   ```

4. Calculez le carré de la différence pour chaque point de données.

   Les carrés pour cet exemple sont les suivants :

   ```
   658.78     215.11    1,626.778
   ```

5. Calculez la somme des carrés :

   La somme des carrés pour cet exemple est 2 500,67.

6. Calculez la somme des carrés, divisée par le nombre de points de données dans le remplissage.

   Le résultat pour cet exemple est 833,56.

7. Calculez la racine carrée de la somme des carrés de la valeur de points de données par rapport à la moyenne de remplissage.

   La racine carrée pour cet exemple est 28,87.

   L'écart type pour cet exemple est 28,87.

Le tableau suivant décrit les moyennes horaires de débit de données par jour, la moyenne des moyennes horaires et l'écart type de remplissage des moyennes horaires pour la même heure :

	Moyennes					
	Lundi	Mardi	Mercredi	...	Moyenne	Écart standard
2 h 00	**76**	**65**	**10**	**...**	**50,33**	**28,87**
3 h 00	87	18	32	...	**45,67**	**29,78**
4 h 00	10	56	40	...	**35,33**	**19,07**
5 h 00	60	45	19	...	**41,33**	**16,94**
Heure ...	...	...	...	...	...	...

Exemple : calcul de la moyenne pour la même heure de la semaine le même jour et de l'écart type de remplissage pour l'utilisation d'UC

L'exemple suivant indique la manière dont la moyenne et l'écart type de remplissage sont calculés pour l'utilisation d'UC sur une unité spécifique, avec trois points de données pour 3 lundis à 02 h 00.

Procédez comme suit :

1. Collectez 3 points de données.

   ```
   Lundi de la semaine :                    1      2      3
   Utilisation d'UC moyenne :    76       4      6
   ```

2. Calculez la moyenne de remplissage.

   La formule de calcul de la moyenne de remplissage est la suivante :

   ```
   La moyenne de remplissage = somme des valeurs de point de données dans le remplissage/nombre de points de données.
   ```

   L'équation pour cet exemple est la suivante :

   ```
   (76+4+6)/3
   Moyenne de remplissage = 28,67.
   ```

3. Calculez la différence entre chaque point de données et la moyenne.

   Les différences pour cet exemple sont les suivantes :

   `47.33  -24.67  -22.67`

4. Calculez le carré de la différence pour chaque point de données.

   Les carrés pour cet exemple sont les suivants :

   `2,240.44  608.44  513.78`

5. Calculez la somme des carrés

   La somme des carrés pour cet exemple est 3 362,67.

6. Calculez la somme des carrés, divisée par le nombre de points de données dans le remplissage.

   Pour cet exemple, le résultat est 1 120,89.

7. Calculez la racine carrée de la somme des carrés de la valeur de points de données par rapport à la moyenne de remplissage.

   La racine carrée pour cet exemple est 33,48.

   L'écart type pour cet exemple est 33,48.

Le tableau suivant décrit les moyennes horaires de débit de données par jour, la moyenne des moyennes horaires et l'écart type de remplissage des moyennes horaires pour le même jour de la semaine, même heure :

	Moyennes							
	Semaine 1		Semaine 2		Semaine 3		Lundi	
	Lundi	...	Lundi	...	Lundi	...	Moyenne	Écart standard
2 h 00	**76**	**...**	**4**	**...**	**6**	**...**	**28,67**	**33,48**
3 h 00	87	...	71	...	56	...	**71,33**	**12,66**
4 h 00	10	...	27	...	58	...	**31,67**	**19,87**
5 h 00	60	...	3	...	32	...	**31,67**	**23,27**
Heure...	...	...	...	...	...	...	...	...

Exemple : calcul de l'écart de la norme à l'aide de la moyenne même heure, même jour de la semaine et de l'écart type de remplissage pour l'utilisation de l'UC

Supposons que Data Aggregator interroge des données d'utilisation d'UC à un intervalle de 5 minutes. Vous définissez une règle d'événement pour générer un événement lorsque l'utilisation de l'UC dépasse un écart type supérieur à la moyenne pour un intervalle d'interrogation unique de 5 minutes.

Dans cet exemple, la durée et la fenêtre sont toutes les deux égales à 5 minutes.

Formule de calcul de la condition de génération d'un événement :

```
Utilisation d'UC = valeur moyenne + 1 (valeur d'écart standard)
```

Par conséquent, pour substituer les valeurs de moyenne et d'écart type à partir du même jour précédent, même heure le lundi à 02 h 00 :

```
Utilisation d'UC = 28,67 + 1 (33,48)
```

```
Utilisation d'UC = 62,15
```

En conséquence, si l'utilisation d'UC dépasse 62,15 pour un intervalle d'interrogation unique de 5 minutes entre 01 h 05 et 02 h 00 le lundi, un événement est généré. Cet événement indique un écart de l'utilisation d'UC par rapport à la normale pour ce délai.

Exemple : analyse des événements d'utilisation d'UC dans une vue Graphique de tendance

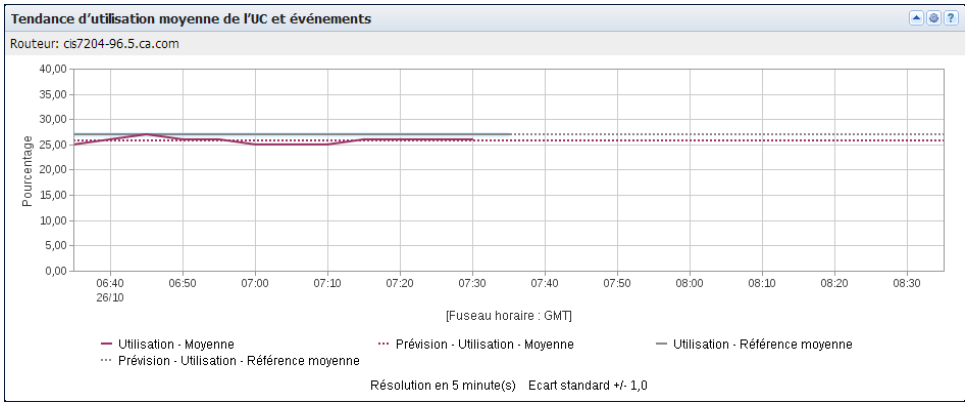
Supposons que Data Aggregator interroge des données d'utilisation d'UC à un intervalle de 5 minutes. Dans cet exemple, vous voulez recevoir une alerte lorsque l'utilisation de l'UC de l'un de vos serveurs critiques pour l'entreprise descend sous le niveau attendu. Vous définissez une règle d'événement pour générer un événement lorsque l'utilisation de l'UC descend sous un écart type inférieure à la moyenne pour un intervalle d'interrogation unique de 5 minutes.

Par exemple, supposez que l'utilisation de l'UC est de 50 %, de lundi 12 h 00 à dimanche 12 h 00. Du dimanche 12 h 00 au lundi 12 h 00, l'utilisation de l'UC est inférieure à 10 %. Cette baisse d'utilisation est attendue. Toutefois, lorsque Data Aggregator commence à calculer la référence moyenne, un événement est renvoyé lorsque l'utilisation de l'UC passe sous les 10 %. L'événement est supprimé lorsque l'utilisation de l'UC repasse le seuil des 50 %. Cet événement erroné est renvoyé car, initialement, lorsqu'une quantité limitée de données est collectée, la référence moyenne est calculée à partir de la même heure de chaque jour et la différence d'utilisation selon les jours de la semaine n'est pas prise en compte. Data Aggregator suppose que l'utilisation de l'UC est *toujours* de 50 %.

Après une période de trois semaines, trois échantillons de données même heure, même jour de la semaine sont disponibles et la méthode de calcul de la référence moyenne change. Data Aggregator définit la norme en faisant la moyenne des échantillons horaires pour le même jour de la semaine. Data Aggregator suppose désormais que l'utilisation de l'UC est de 10 % pour toutes les périodes comprises entre le dimanche 12 h 00 et le lundi 12 h 00. L'événement erroné renvoyé précédemment tous les dimanches à 12 h 00 ne l'est plus.

La vue suivante présente la méthode de calcul initiale de la référence moyenne pour la même heure de chaque jour. Lorsque des données supplémentaires sont disponibles, un basculement de la méthode de calcul se produit automatiquement. Data Aggregator établit la moyenne des échantillons horaires pour le même jour de la semaine.

Cette vue indique également que les événements erronés ne sont plus renvoyés lorsque la méthode de calcul est modifiée.



Calculs du 95e centile

Le 95e centile est calculé pour les cumuls et à des fins de génération de rapports et d'événements.

Cumuls :

- Pour des cumuls horaires, le 95e centile est calculé comme un centile continu des valeurs interrogées.
- Pour des cumuls quotidiens, le 95e centile est calculé comme un centile continu du 95e centile horaire.
- Pour des cumuls hebdomadaires et au-delà, le 95e centile est calculé comme centile continu du 95e centile quotidien.

Génération de rapports :

- Lorsque la résolution est inférieure à un jour, le 95e centile est calculé comme un centile continu des valeurs interrogées.
- Lorsque la résolution est d'un jour ou plus, le 95e centile est calculé comme le 95e du 95e.

Exemple : Calcul du 95e centile

L'exemple suivant présente le calcul du 95e centile; compte tenu d'une heure de calcul et d'un cycle de sondage de 5 minutes.

Procédez comme suit :

1. Collectez une heure de données à un cycle de sondage de 5 minutes.

   1 2 3 4 5 6 7 8 9 10 11 12

   30 10 20 70 60 30 80 10 90 20 70 50

   Réorganisez.

   10 10 20 20 30 30 50 60 70 70 80 90

2. Calculez les valeurs de numéro de ligne (RN), de numéro de ligne de plancher (FRN) et de numéro de ligne de plafond (CRN).

   Les formules permettant de calculer les valeurs RN, FRN, et CRN sont les suivantes :

   - RN = 1+((N-1)*P)

     N

     Représente le nombre de valeurs interrogées qui ont été collectées.

     P

     Représente la valeur de centile.

   - FRN = plancher (RN)

     FRN

     Représente le plus grand nombre entier qui n'est pas supérieur à RN.

   - CRN = plafond (RN)

     CRN

     Représente le plus petit nombre entier qui n'est pas inférieur à RN.

   Les équations pour cet exemple sont les suivantes :

   ```
   RN = 1+((12-1)*0.95) = 11.45
   FRN = plancher (RN) = 11
   CRN = plafond (RN) = 12
   ```

3. Calculez le 95e centile

   La formule de calcul du 95e centile est la suivante :

   ```
   si (CRN = FRN = RN) alors
   (valeur d'expression à partir de ligne à RN)
   else
   (valeur d'expression pour la ligne à FRN) + (RN - FRN) * (ligne CRN - valeur de ligne FRN)
   ```

   L'équation pour cet exemple est la suivante :

   ```
   (80) + (11.45 - 11)*(90-80) = 84.5000
   ```

   Le 95e centile pour cet exemple est 84.5000.

Calculs d'écart standard

L'écart type est calculé pour les cumuls et à des fins de génération de rapports et d'événements.

Cumuls :

- Pour des cumuls horaires, l'écart standard est calculé pour les valeurs interrogées.
- Pour des cumuls quotidiens, l'écart standard est calculé pour des moyennes horaires.
- Pour des cumuls hebdomadaires et au-delà, l'écart standard est calculé pour les moyennes quotidiennes.

Evénements :

- L'écart type fournit un indicateur statistique du degré de variabilité qui existe au niveau des données de remplissage qui interviennent dans le calcul de la référence moyenne.

Génération de rapports :

- Pour des rapports horaires, l'écart standard est calculé pour les valeurs interrogées.
- Pour des rapports quotidiens, l'écart standard est calculé pour des moyennes horaires.
- Pour des rapports hebdomadaires et au-delà, l'écart standard est calculé pour les moyennes quotidiennes.

Exemple : Calcul de l'écart standard de remplissage.

L'exemple suivant présente la manière dont l'écart standard de remplissage est calculé, compte tenu de 12 points de données.

Le *remplissage* fait référence à un ensemble de valeurs potentielles, comprenant non seulement les cas qui sont observés, mais aussi ceux qui sont potentiellement observables.

La formule permettant de calculer cet écart standard est la suivante :

écart de remplissage = racine carrée de (somme (X - remplissage moyen)/nombre de points de données)

X

est la valeur de point de données dans le remplissage.

Procédez comme suit :

1. Collectez 12 points de données.

   1 2 3 4 5 6 7 8 9 10 11 12

   30 10 20 70 60 30 80 10 90 20 70 50

2. Calculez la moyenne de remplissage.

   La moyenne de remplissage = somme des valeurs de point de données dans le remplissage/nombre de points de données.

   La moyenne de remplissage pour cet exemple est de 45.

3. Calculez la différence entre chaque point de données et la moyenne.

   Les différences pour cet exemple sont les suivantes :

   -15 -35 -25 25 15 -15 35 -35 45 -25 25 5

4. Calculez le carré de la différence pour chaque point de données.

   Les carrés pour cet exemple sont les suivants :

   225 1225 625 625 225 225 1225 1225 2025 625 625 25

5. Calculez la somme des carrés :

   La somme des carrés pour cet exemple est 8900.

6. Calculez la somme des carrés, divisée par le nombre de points de données dans le remplissage.

   La moyenne de remplissage pour cet exemple est de 741,6666667.

7. Calculez la racine carrée de la somme des carrés de la valeur de points de données par rapport à la moyenne de remplissage.

   La racine carrée pour cet exemple est de 27,23355773.

   L'écart standard pour cet exemple est de 27,23355773.

Annexe B: Dépannage

Ce chapitre traite des sujets suivants :

Dépannage : la détection ne démarre pas (page 169)
Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée (page 170)
Dépannage : message d'événement d'arrêt de l'interrogation (page 171)
Dépannage : l'interrogation ne termine pas pour une unité primordiale (page 171)
Dépannage : modification de l'adresse IP de Data Aggregator requise pour la modification de mon environnement (page 172)
Dépannage : arrêt inattendu de Data Aggregator (page 172)
Dépannage : je ne parviens pas à sauvegarder le Data Repository. (page 174)
Dépannage : Déclenchement d'alarmes d'intrusion en cas de présence de plusieurs unités SNMP (page 175)

Dépannage : la détection ne démarre pas

Symptôme :

Lorsque vous sélectionnez les profils de détection et cliquez sur Exécuter pour exécuter une détection, la détection ne démarre pas ou le bouton Exécuter est désactivé.

Solution :

Les raisons possibles d'un échec de détection ou de la désactivation du bouton Exécuter sont les suivantes :

- Le domaine IP préalablement spécifié dans le profil de détection a été supprimé. Affectation du profil de détection à un domaine IP.
- Aucune instance de Data Collector n'a été installée pour le domaine IP spécifié dans le profil de détection sélectionné.

  Remarque : Pour plus d'informations sur l'installation des hôtes *Data Collector*, reportez-vous au *Manuel d'installation de Data Aggregator*.
- Un ou plusieurs hôtes Data Collector sont installés pour le domaine IP spécifié dans le profil de détection sélectionné. Toutefois, tous les hôtes Data Collector qui sont installés pour le domaine IP sont arrêtés. Démarrez les hôtes Data Collector.
- Le client hébergé est désactivé. Activez le client hébergé.

Informations complémentaires :

Modification des profils de détection (page 73)
Activation des clients hébergés (page 109)

Dépannage : l'interrogation s'est arrêtée sur la famille de mesures détectée

Symptôme :

Je sélectionne une unité dans la page Unités surveillées et je constate qu'une famille de mesures prise en charge par l'unité a cessé l'interrogation. Je n'avais pas l'intention d'arrêter l'interrogation pour cette famille de mesures.

Solution :

Procédez comme suit pour déterminer pourquoi l'interrogation a cessé et prendre les mesures appropriées pour résoudre la cause :

1. Vérifiez qu'un profil de surveillance est défini et prêt à interroger la famille de mesures souhaitée (page 90).

   Si cette exigence n'est pas déjà satisfaite, créez ou modifiez un profil de surveillance contenant la famille de mesures souhaitée.

2. Vérifiez que l'unité est associée à la collection (page 93).

   Si l'unité n'est pas associée à la collection d'unités, ajoutez-la à la collection.

   Remarque : Pour plus d'informations sur l'ajout d'une unité à une collection, reportez-vous au *Manuel de l'administrateur de CA Performance Center*.

3. Vérifiez que le profil de surveillance est associé à la collection d'unités et à l'unité (page 90).

   Si le profil de surveillance n'est pas associé, créez la relation entre le profil de surveillance et la collection d'unités (page 92).

Après avoir terminé l'une de ces actions pour redémarrer l'interrogation, sélectionnez l'unité dans la page Unités surveillées pour vérifier :

- Le statut de la famille de mesures indiquée dans l'onglet Familles de mesures interrogées a changé.
- Le statut indiqué dans le tableau Composants d'interface est passé à Actif.

L'interrogation reprend automatiquement sur les unités existantes.

Il est possible de détecter de nouvelles unités en suivant une des méthodes suivantes :

- Sélectionnez la famille de mesures interrogée dans la page Unités surveillées, puis cliquez sur Mettre à jour la famille de mesures (page 99).
- Définissez le taux de détection des modifications dans le profil de surveillance pour cette famille de mesures, avec la détection automatique définie sur True.

Dépannage : message d'événement d'arrêt de l'interrogation

Symptôme :

Un événement "interrogation arrêtée" s'affiche dans ma liste des événements. Pourquoi ?

Solution :

Par défaut, Data Aggregator contrôle l'interrogation SNMP, ce qui permet d'empêcher qu'un nombre excessif de demandes d'interrogation envahisse une unité. Le seuil de délais d'expiration SNMP est une méthode de contrôle du trafic d'interrogation. La valeur limite par défaut est 15. Par conséquent, lorsque 15 demandes SNMP ou plus expirent, l'interrogation est suspendue pour le reste du cycle d'interrogation en cours. Un événement est généré, vous informant de la situation.

Remarque : L'interrogation reprend au début de chaque cycle d'interrogation. Lorsqu'aucun délai d'expiration ne se produit dans un cycle d'interrogation complet de 5 minutes, un événement "d'effacement" est généré.

Dépannage : l'interrogation ne termine pas pour une unité primordiale

Symptôme :

J'utilise une unité critique que je dois surveiller, or l'interrogation ne peut pas terminer dans un cycle d'interrogation unique. Le trafic réseau est parfois tellement élevé que mon unité s'arrête complètement. Cette unité est critique. Comment puis-je l'interroger de façon fiable pour garantir des performances optimum ?

Solution :

L'interrogation est cruciale pour surveiller une unité. Toutefois, un nombre trop élevé d'interrogations peut entraîner un trafic réseau trop élevé et peut détériorer votre capacité à surveiller une unité. Si le trafic réseau sature votre unité critique, vous pouvez effectuer les réglages suivants afin de réduire le trafic global dans l'unité :

- Ajustez votre profil de surveillance pour exclure les familles de mesures non indispensables de l'interrogation.
- Appliquez un filtre dans votre profil de surveillance pour réduire le nombre d'interfaces interrogées.
- Ajustez votre profil de surveillance pour interroger à une fréquence inférieure (par exemple, définissez la fréquence d'interrogation SNMP sur 15 minutes, plutôt que les 5 minutes par défaut).

- Ajustez le seuil de trafic SNMP pour réduire le nombre de demandes SNMP envoyées à l'unité.
- Ajustez le seuil d'expiration SNMP pour contrôler le nombre d'expirations de l'interrogation devant aboutir sur la suspension de l'interrogation pendant le cycle d'interrogation actuel.

Dépannage : modification de l'adresse IP de Data Aggregator requise pour la modification de mon environnement

Symptôme :

Modification de l'adresse IP de Data Aggregator requise pour la modification de mon environnement

Solution :

Pour modifier l'adresse IP de Data Aggregator, procédez comme suit :

1. Arrêtez le composant Data Aggregator en vous connectant, en tant qu'utilisateur root, à l'ordinateur sur lequel il est installé. Saisissez la commande suivante :

   ```
   service dadaemon stop
   ```

   Le Data Aggregator s'arrête.

2. Saisissez la commande suivante pour accéder au répertoire jms :

   cd *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/jms

3. Modifiez le fichier local-jms-broker.xml dans un éditeur tel que vi. Remplacez l'adresse IP qui s'affiche dans la partie inférieure de ce fichier par celle de votre choix.

4. Redémarrez le composant Data Aggregator en vous connectant, en tant qu'utilisateur root, à l'ordinateur sur lequel il est installé. Ouvrez une invite de commande et saisissez la commande suivante :

   ```
   service dadaemon start
   ```

   Data Aggregator démarre. L'adresse IP de Data Aggregator est modifiée.

Dépannage : arrêt inattendu de Data Aggregator

Symptôme :

Data Aggregator se ferme de manière inattendue.

Solution :

Le Data Aggregator se ferme lorsqu'il perd le contact avec le Data Repository. Si la communication avec le Data Repository est perdue, un message d'audit est journalisé dans le fichier *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/shutdown.log

Remarque : Le fichier *répertoire d'installation de Data Aggregator*/apache-karaf-2.3.0/shutdown_details.log journalise les messages de signal d'activité échangés entre Data Aggregator et Data Repository, ainsi que les arrêts de Data Aggregator à des fins de débogage.

Pour résoudre les problèmes liés à la connectivité ou au Data Repository, procédez comme suit :

1. Vérifiez que le Data Repository est en cours d'exécution. Procédez comme suit :
    a. Connectez-vous au serveur de base de données que vous utilisez pour le Data Repository en tant qu'administrateur de base de données et non pas qu'utilisateur root :
    b. Saisissez la commande suivante :

        ```
        /opt/vertica/bin/adminTools
        ```

        La boîte de dialogue Administration Tools s'affiche.
    c. Sélectionnez (1) View Database Cluster State.

        La fenêtre qui s'affiche devrait indiquer l'hôte ALL et pour l'état UP.
2. Si le Data Repository ne s'exécute pas, essayez de le démarrer en procédant comme suit :
    a. Connectez-vous au serveur de base de données que vous utilisez pour le Data Repository.
    b. Saisissez les commandes suivantes :

        ```
        /opt/vertica/bin/adminTools
        ```

        La boîte de dialogue Administration Tools s'affiche.
    c. Sélectionnez (3) Démarrer la base de données.
    d. Appuyez sur la barre d'espacement à côté du nom de la base de données, sélectionnez **OK** et appuyez sur Entrée.

        Vous êtes invité à entrer le mot de passe de la base de données.

e. Entrez le mot de passe de base de données et appuyez sur Entrée.

   La base de données Data Repository s'arrête.

   Remarque : Si un message d'erreur s'affiche spécifiant que vous ne pouvez pas vous connecter à cause d'une erreur au niveau du nom d'utilisateur ou du mot de passe, cela indique peut-être que le Data Aggregator s'est déconnecté du Data Repository suite à la modification du mot de passe de la base de données.

f. Sélectionnez (E) Quitter et appuyez sur Entrée.

   Si le Data Repository ne démarre pas, contactez le support technique de CA.

3. L'exécution du Data Repository indique qu'un problème a lieu au niveau de la connexion au réseau, un problème de latence du réseau par exemple. Résolvez ce problème de connectivité réseau.
4. Une fois Data Aggregator de nouveau en cours d'exécution, configurez une récupération automatique du processus Data Aggregator.

   Remarque : Pour plus d'informations sur la configuration de la récupération automatique du processus Data Aggregator, consultez le *Manuel d'installation de Data Aggregator*.

Dépannage : je ne parviens pas à sauvegarder le Data Repository.

Symptôme :

Lorsque j'exécute le script vbr.py pour sauvegarder le Data Repository, le message "Another vbr instance is already running" (une autre instance de vbr est déjà en cours d'exécution) s'affiche.

Solution :

Ce message indique qu'une tentative de sauvegarde précédente a échoué pour l'une des nombreuses raisons possibles (par exemple, le fichier ssh sans mot de passe n'a pas été configuré correctement).

Pour réessayer de sauvegarder le Data Repository, procédez comme suit :

1. Supprimez le fichier /tmp/.initiator.mutex de l'ordinateur sur lequel le Data Repository que vous souhaitez sauvegarder est installé.

   La sauvegarde planifiée suivante se produira normalement.

Dépannage : Déclenchement d'alarmes d'intrusion en cas de présence de plusieurs unités SNMP

Symptôme :

Un grand nombre d'unités SNMP sont placées derrière une configuration de pare-feu plus restreinte (des réseaux de zone DMZ par exemple). Pour des raisons de sécurité, les chaînes de communauté des unités SNMP sont différentes. J'ai défini un profil SNMP pour chaque chaîne de communauté, mais maintenant j'obtiens des alarmes d'intrusion et ai été déconnecté de CA Performance Center.

Solution :

Pour trouver le profil SNMP approprié pour une unité, CA Performance Center essaie tous les profils SNMP. Ce comportement peut déclencher des alarmes d'intrusion et peut entraîner votre déconnexion de CA Performance Center.

Pour résoudre ce problème, procédez comme suit :

1. Créez un profil de détection distinct pour chaque unité SNMP critique.
2. Affectez le profil SNMP avec la chaîne de communauté appropriée au profil de détection.
3. Répétez les étapes un et deux pour chaque unité SNMP critique.

Lorsque la détection a lieu, seul le profil SNMP affecté est utilisé.

Glossaire

Collection d'unités

Une *collection d'unités* est un groupement logique d'unités surveillées, telles que des serveurs ou des routeurs.

cumul

Un *cumul* est le processus au cours duquel les valeurs de mesure sont cumulées. Dans un cumul horaire, les valeurs interrogées à la minute 1, la minute 5, à la minute 15, à la minute 30 et à la minute 60 pour les mesures sont cumulées toutes les heures. Dans un cumul quotidien, les valeurs horaires des mesures sont cumulées une fois par jour. Dans un cumul hebdomadaire, les valeurs quotidiennes des mesures sont cumulées une fois par semaine.

Data Collector

Data Collector coordonne la collecte des données et interroge activement les données qui sont utilisées pour la génération de rapports et l'analyse d'événements. Les mesures opérationnelles et les données de configuration sont interrogées sur des unités détectées et leurs composants surveillés. Les données collectées sont transmises via Data Aggregator et stockées dans le Data Repository.

écart standard

L'écart standard indique l'écart par rapport à la moyenne (valeur moyenne ou attendue). Un écart standard bas indique que les points de données tendent à être très proches de la moyenne. Un écart standard élevé indique que les points de données s'étendent sur une large plage de valeurs.

élément

Un *élément* peut être une unité, un composant ou une interface surveillés par Data Aggregator.

Famille de mesures

Une *famille de mesures* définit l'ensemble de valeurs permettant de collecter et de générer des rapports pour une technologie donnée. Ces valeurs sont normalisées afin d'uniformiser la génération de rapports indépendamment de la source de données. Lorsqu'elles sont incluses dans un profil de surveillance, les familles de mesures déterminent quelles valeurs collecter pour les unités associées à ce profil de surveillance.

Prédéfini

Le terme "*prédéfini*" dans Data Aggregator décrit des éléments que CA Technologies fournit. Ils sont souvent installés avec le produit. Par exemple, Data Aggregator fournit des certifications de fournisseur prédéfinies, des profils de surveillance prédéfinis, et bien plus encore. Ces éléments préconfigurés peuvent vous aider à rendre Data Aggregator opérationnel dès son installation. Ils peuvent également servir d'exemples pour créer ou importer des versions personnalisées du même élément. Plus important encore, les utilisateurs de Data Aggregator ne peuvent pas modifier ces éléments prédéfinis.

Profil de détection

Un *profil de détection* spécifie le mode de détection de l'inventaire, y compris les adresses IP, les plages d'adresse IP et les noms d'hôte utilisés pour localiser les unités.

profil de surveillance

Un *profil de surveillance* est associé à une collection d'unités pour spécifier les informations à interroger et le taux d'interrogation. Ces paramètres sont appliqués à chaque unité de la collection. Une sélection de profils de surveillance par défaut basés sur des types d'unités (tels que les routeurs, les commutateurs et les serveurs) est fournie..
Le profil de surveillance contient également les règles d'événement qui sont appliquées à chaque élément d'unité dans la collection d'unités associée. Les évaluations de règle sont appliquées à chaque élément d'unité de la collection d'unités et à chaque mesure que vous spécifiez dans les règles d'événement. Ces évaluations de règle génèrent la création ou l'effacement d'événements. Ces événements sont alors envoyés au gestionnaire d'événements dans CA Performance Center, CA Spectrum et dans l'outil de notification de CA Performance Center pour toute action supplémentaire.

Références moyennes

Selon la quantité des données interrogées qui sont collectées, les *moyennes de référence* sont calculées de deux façons :

- Initialement, la moyenne des moyennes horaires pour la même heure est calculée (indépendamment du jour).
- Une fois qu'un nombre suffisant de données est collecté, la moyenne des moyennes horaires même jour, même heure est calculée.

Les moyennes de référence permettent d'indiquer les performances pour les mesures surveillées sélectionnées et d'évaluer des performances actuelles. Les références moyennes et les écarts types associés sont calculés toutes les heures de manière continue. L'écart type fournit un indicateur statistique du degré de variabilité qui existe au niveau des données de remplissage qui interviennent dans le calcul de la référence moyenne.

Dans Data Aggregator, la valeur de base pour une durée spécifiée dans une fenêtre de temps correspond à la moyenne de référence calculée.

Surveillance du 95e centile

La surveillance du 95e centile se rapporte à la bande passante. Cette statistique est utile pour mesurer le débit de données car elle reflète de façon plus précise la capacité requise du lien surveillé pour les applications sensibles à la bande passante. Le 95e centile indique que 95 % du temps, l'utilisation de la bande passante est inférieure à cette quantité. Les 5 % de restants, l'utilisation de la bande passante est supérieure cette quantité.